ID: 876998
Sample Name: 01860199.exe
Cookbook: default.jbs
Time: 10:41:06
Date: 28/05/2023
Version: 37.1.0 Beryl

Table of Contents

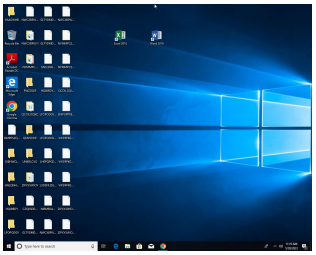
Windows Analysis Report

01860199.exe

Overview

General Information

Sample Name:	01860199.exe
Analysis ID:	876998
MD5:	3d8207e1ce67…
SHA1:	82a02d6e00de…
SHA256:	c38267836dde…
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

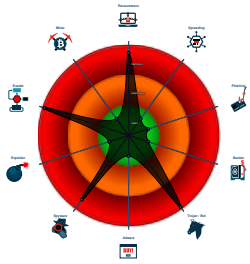
Amadey, Babuk, Clipboard Hijacker, Djvu, Fabookie, SmokeLoader, Vidar

Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Amadeys stealer DLL
- Detected unpacking (overwrites its o…
- Found ransom note / readme
- Yara detected Babuk Ransomware
- Yara detected SmokeLoader
- Yara detected Amadey bot
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Yara detected Clipboard Hijacker
- Snort IDS alert for network traffic

Classification



Process Tree

- **System is w10x64**
- 01860199.exe (PID: 1264 cmdline: C:\Users\user\Desktop\01860199.exe MD5: 3D8207E1CE6762FF10DB118BEE3BD99B)
  - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - D804.exe (PID: 2560 cmdline: C:\Users\user\AppData\Local\Temp\D804.exe MD5: 6944FCA258A9009F9D3B7212CDB4874D)
      - D804.exe (PID: 772 cmdline: C:\Users\user\AppData\Local\Temp\D804.exe MD5: 6944FCA258A9009F9D3B7212CDB4874D)
        - icacls.exe (PID: 4704 cmdline: icacls "C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e" /deny *S-1-1-0:(OI)(CI)(DE,DC) MD5: FF0D1D4317A44C951240FAE75075D501)
        - D804.exe (PID: 128 cmdline: "C:\Users\user\AppData\Local\Temp\D804.exe" --Admin IsNotAutoStart IsNotTask MD5: 6944FCA258A9009F9D3B7212CDB4874D)
          - D804.exe (PID: 4528 cmdline: "C:\Users\user\AppData\Local\Temp\D804.exe" --Admin IsNotAutoStart IsNotTask MD5: 6944FCA258A9009F9D3B7212CDB4874D)
            - build2.exe (PID: 4696 cmdline: "C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe" MD5: B888EFE68F257AA2335ED9CBD63C1343)
              - build2.exe (PID: 6096 cmdline: "C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe" MD5: B888EFE68F257AA2335ED9CBD63C1343)
            - build3.exe (PID: 5868 cmdline: "C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build3.exe" MD5: 9EAD10C08E72AE41921191F8DB39BC16)
              - schtasks.exe (PID: 5268 cmdline: /C /create /F /sc mi nute /mo 1 /tn "Azure-Update-Task" /tr " C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe" MD5: 15FF7D8324231381BAD48A052F85DF04)
                - conhost.exe (PID: 5228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - C861.exe (PID: 68 cmdline: C:\Users\user\AppData\Local\Temp\C861.exe MD5: 7A8E3D000FBA0F5765B98E2D78EB9D12)
      - WerFault.exe (PID: 5568 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 68 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 1868 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 508 -p 68 -ip 68 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - 3C54.exe (PID: 1720 cmdline: C:\Users\user\AppData\Local\Temp\3C54.exe MD5: 2AF03D52F9CF9E53DFFC1183B403E1B7)
      - aafg31.exe (PID: 2336 cmdline: "C:\Users\user\AppData\Local\Temp\aafg31.exe" MD5: B4F79B3194235084A3EC85711EDFBD38)
      - NewPlayer.exe (PID: 4364 cmdline: "C:\Users\user\AppData\Local\Temp\NewPlayer.exe" MD5: 08240E71429B32855B418A4ACF0E38EC)
        - mnolyk.exe (PID: 5348 cmdline: "C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe" MD5: 08240E71429B32855B418A4ACF0E38EC)
      - XandETC.exe (PID: 5320 cmdline: "C:\Users\user\AppData\Local\Temp\XandETC.exe" MD5: 3006B49F3A30A80BB85074C279ACC7DF)
    - B46F.exe (PID: 4928 cmdline: C:\Users\user\AppData\Local\Temp\B46F.exe MD5: 6944FCA258A9009F9D3B7212CDB4874D)
      - B46F.exe (PID: 2576 cmdline: C:\Users\user\AppData\Local\Temp\B46F.exe MD5: 6944FCA258A9009F9D3B7212CDB4874D)
    - A170.exe (PID: 1868 cmdline: C:\Users\user\AppData\Local\Temp\A170.exe MD5: 15BC205C2CAF7196EE2267087C3B2BB8)
      - A170.exe (PID: 1964 cmdline: C:\Users\user\AppData\Local\Temp\A170.exe MD5: 15BC205C2CAF7196EE2267087C3B2BB8)
    - D804.exe (PID: 1264 cmdline: "C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe" --AutoStart MD5: 6944FCA258A9009F9D3B7212CDB4874D)
    - 913F.exe (PID: 5260 cmdline: C:\Users\user\AppData\Local\Temp\913F.exe MD5: 15BC205C2CAF7196EE2267087C3B2BB8)
      - 913F.exe (PID: 5512 cmdline: C:\Users\user\AppData\Local\Temp\913F.exe MD5: 15BC205C2CAF7196EE2267087C3B2BB8)

- F4F7.exe (PID: 5436 cmdline: C:\Users\user\AppData\Local\Temp\F4F7.exe MD5: 7A8E3D000FBA0F5765B98E2D78EB9D12)
- 5DA0.exe (PID: 6404 cmdline: C:\Users\user\AppData\Local\Temp\5DA0.exe MD5: 2AF03D52F9CF9E53DFFC1183B403E1B7)
- D804.exe (PID: 5444 cmdline: "C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe" --AutoStart MD5: 6944FCA258A9009F9D3B7212CDB4874D)
- hwgujdv (PID: 5940 cmdline: C:\Users\user\AppData\Roaming\hwgujdv MD5: 3D8207E1CE6762FF10DB118BEE3BD99B)
- D804.exe (PID: 1340 cmdline: C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe --Task MD5: 6944FCA258A9009F9D3B7212CDB4874D)
  - D804.exe (PID: 6088 cmdline: C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe --Task MD5: 6944FCA258A9009F9D3B7212CDB4874D)
- mstsca.exe (PID: 6600 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe MD5: 9EAD10C08E72AE41921191F8DB39BC16)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Amadey	Amadey is a botnet that appeared around October 2018 and is being sold for about $500 on Russian-speaking hacking forums. It periodically sends information about the system and installed AV software to its C2 server and polls to receive orders from it. Its main functionality is that it can load other payloads (called "tasks") for all or specifically targeted computers compromised by the malware.	No Attribution	http://https://asec.ahnlab.com/en/36634/https://asec.ahnlab.com/en/41450/https://asec.ahnlab.com/en/44504/https://blog.cyble.com/2023/01/25/the-rise-of-amadey-bot-a-growing-concern-for-internet-security/https://blog.minerva-labs.com/underminer-exploit-kit-the-more-you-check-the-more-evasive-you-become	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.amadey

Name	Description	Attribution	Blogpost URLs	Link
Babuk	Babuk Ransomware is a sophisticated ransomware compiled for several platforms. Windows and ARM for Linux are the most used compiled versions, but ESX and a 32bit old PE executable were observed over time. as well It uses an Elliptic Curve Algorithm (Montgomery Algorithm) to build the encryption keys.	No Attribution	http://chuongdong.com/reverse%20engineering/2021/01/03/BabukRansomware/https://blog.cyble.com/2022/05/06/rebranded-babuk-ransomware-in-action-darkangels-ransomware-performs-targeted-attack/https://blog.morphisec.com/babuk-ransomware-variant-major-attackhttps://blog.talosintelligence.com/2021/11/babuk-exploits-exchange.htmlhttps://chuongdong.com/reverse%20engineering/2021/01/16/BabukRansomware-v3/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.babuk

Name	Description	Attribution	Blogpost URLs	Link
STOP, Djvu	STOP Djvu Ransomware it is a ransomware which encrypts user data through AES-256 and adds one of the dozen available extensions as marker to the encrypted file's name. It is not used to encrypt the entire file but only the first 5 MB. In its original version it was able to run offline and, in that case, it used a hard-coded key which could be extracted to decrypt files.	No Attribution	http://https://angle.ankura.com/post/102het9/the-stop-ransomware-varianthttps://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/https://cybergeeks.tech/a-detailed-analysis-of-the-stop-djvu-ransomware/https://cybleinc.com/2021/06/21/djvu-malware-of-stop-ransomware-family-back-with-new-variant/https://github.com/vithakur/detections/blob/main/STOP-ransomware-djvu/IOC-list	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.stop

Name	Description	Attribution	Blogpost URLs	Link
Fabookie	Fabookie is facebook account info stealer.	No Attribution	http://https://ics-cert.kaspersky.com/publications/reports/2021/12/16/pseudomanuscrypt-a-mass-scale-spyware-attack-campaign/https://medium.com/@lcam/updates-from-the-maas-new-threats-delivered-through-nullmixer-d45defc260d1	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.fabookie

Name	Description	Attribution	Blogpost URLs	Link
SmokeLoader	The SmokeLoader family is a generic backdoor with a range of capabilities which depend on the modules included in any given build of the malware. The malware is delivered in a variety of ways and is broadly associated with criminal activity. The malware frequently tries to hide its C2 activity by generating requests to legitimate sites such as microsoft.com, bing.com, adobe.com, and others. Typically the actual Download returns an HTTP 404 but still contains data in the Response Body.	• SMOKY SPIDER	http://security.neurolabs.club/2019/08/smokeloaders-hardcoded-domains-sneaky.htmlhttp://security.neurolabs.club/2019/10/dynamic-imports-and-working-around.htmlhttp://security.neurolabs.club/2020/04/diffing-malware-samples-using-bindiff.htmlhttp://security.neurolabs.club/2020/06/unpacking-smokeloader-and.htmlhttps://0xc0decafe.com/2020/12/23/detect-rc4-in-malicious-binaries	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.smokeloader

Name	Description	Attribution	Blogpost URLs	Link
Vidar	Vidar is a forked malware based on Arkei. It seems this stealer is one of the first that is grabbing information on 2FA Software and Tor Browser.	No Attribution	http://https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-1-(-Unpacking-)/https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-2/https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/vidar-stealer-h-and-m-campaignhttps://0xtoxin.github.io/malware%20analysis/Vidar-Stealer-Campaign/https://asec.ahnlab.com/en/22932/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar

Malware Configuration

Threatname: Amadey


```
{
  "C2 url": "45.9.74.80/0bjdn2Z/index.php",
  "Version": "3.67"
}
```


Threatname: Djvu


```
{
  "Download URLs": [
    "http://colisumy.com/dl/build2.exe",
    "http://zexeq.com/files/1/build3.exe"
  ],
  "C2 url": "http://zexeq.com/raud/get.php",
  "Ransom note file": "_readme.txt",
  "Ransom note": "ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.\r\nThe only method of recovering files is to purchase decrypt tool and unique key for you.\r\nThis software will decrypt all your encrypted files.\r\nWhat guarantees you have?\r\nYou can send one of your encrypted file from your PC and we decrypt it for free.\r\nBut we can decrypt only 1 file for free. File must not contain valuable information.\r\nYou can get and look video overview decrypt tool:\r\nhttps://we.tl/t-tnzomMj6HU\r\nPrice of private key and decrypt software is $980.\r\nDiscount 50% available if you contact us first 72 hours, that's price for you is $490.\r\nPlease note that you'll never restore your data without payment.\r\nCheck your e-mail \"Spam\" or \"Junk\" folder if you don't get answer more than 6 hours.\r\n\r\n\r\nTo get this software you need write on our e-mail:\r\nsupport@freshmail.top\r\n\r\nReserve e-mail address to contact us:\r\ndatarestorehelp@airmail.cc\r\n\r\nYour personal ID:\r\n0717JOsie",
  "Ignore Files": [
    "ntuser.dat",
    "ntuser.dat.LOG1",
    "ntuser.dat.LOG2",
    "ntuser.pol",
    ".sys",
    ".ini",
    ".DLL",
    ".dll",
    ".blf",
    ".bat",
    ".lnk",
    ".regtrans-ms",
    "C:||SystemID||",
    "C:||Users||Default User||",
    "C:||Users||Public||",
    "C:||Users||All Users||",
    "C:||Users||Default||",
    "C:||Documents and Settings||",
    "C:||ProgramData||",
```

```
    "C:||Recovery||",
    "C:||System Volume Information||",
    "C:||Users||%username%||AppData||Roaming||",
    "C:||Users||%username%||AppData||Local||",
    "C:||Windows||",
    "C:||PerfLogs||",
    "C:||ProgramData||Microsoft||",
    "C:||ProgramData||Package Cache||",
    "C:||Users||Public||",
    "C:||$Recycle.Bin||",
    "C:||$WINDOWS.~BT||",
    "C:||dell||",
    "C:||Intel||",
    "C:||MSOCache||",
    "C:||Program Files||",
    "C:||Program Files (x86)||",
    "C:||Games||",
    "C:||Windows.old||",
    "D:||Users||%username%||AppData||Roaming||",
    "D:||Users||%username%||AppData||Local||",
    "D:||Windows||",
    "D:||PerfLogs||",
    "D:||ProgramData||Desktop||",
    "D:||ProgramData||Microsoft||",
    "D:||ProgramData||Package Cache||",
    "D:||Users||Public||",
    "D:||$Recycle.Bin||",
    "D:||$WINDOWS.~BT||",
    "D:||dell||",
    "D:||Intel||",
    "D:||MSOCache||",
    "D:||Program Files||",
    "D:||Program Files (x86)||",
    "D:||Games||",
    "E:||Users||%username%||AppData||Roaming||",
    "E:||Users||%username%||AppData||Local||",
    "E:||Windows||",
    "E:||PerfLogs||",
    "E:||ProgramData||Desktop||",
    "E:||ProgramData||Microsoft||",
    "E:||ProgramData||Package Cache||",
    "E:||Users||Public||",
    "E:||$Recycle.Bin||",
    "E:||$WINDOWS.~BT||",
    "E:||dell||",
    "E:||Intel||",
    "E:||MSOCache||",
    "E:||Program Files||",
    "E:||Program Files (x86)||",
    "E:||Games||",
    "F:||Users||%username%||AppData||Roaming||",
    "F:||Users||%username%||AppData||Local||",
    "F:||Windows||",
    "F:||PerfLogs||",
    "F:||ProgramData||Desktop||",
    "F:||ProgramData||Microsoft||",
    "F:||Users||Public||",
    "F:||$Recycle.Bin||",
    "F:||$WINDOWS.~BT||",
    "F:||dell||",
    "F:||Intel||"
  ],
  "Public Key": "-----BEGIN PUBLIC KEY-----
||||nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA50iTgpK4WqHRCxsCP+Ko||||ni6Rfb9WWM4K||/vgKVvZi||/+pA7wR6QvFBURdJ1Z9mdw8kYkafMfVuTEgbW+j4RDepy||||nRMc6ZcYdxsu2f4+XgrCWmwJw8wVmod
WyLZqqeb1k4FONQs+uAP0AxLLTUbcAfP75||||ngGAW9KhqPhoYKVhzDqtFOqCvYqMylrgCNwHpTp75Bv5up3OfAE5h6+t||/TfjQjDFJ||||nJY0Tgum721KiGGppZfsBDqY1Zv||/F45h+MVk9mhfvBd3UZNJUZI5ewP1zbnOU1llz|
|||ndETA6WbQWWm4u4pamw3U0ZLnFDJQkUgOAbxOfVM4xpi0lrPyV+oTCXnpOgcF4YvU||||n2wIDAQAB||||n-----END PUBLIC KEY-----"
}
```


Threatname: SmokeLoader


```
{
  "Version": 2022,
  "C2 list": [
    "http://toobussy.com/tmp/",
    "http://wuc11.com/tmp/",
    "http://ladogatur.ru/tmp/",
    "http://kingpirate.ru/tmp/"
  ]
}
```


Threatname: Vidar

```
{
  "C2 url": [
    "https://steamcommunity.com/profiles/76561199508624021",
    "https://t.me/looking_glassbot"
  ],
  "Botnet": "e44c96dfdf315ccf17cdd4b93cfe6e48"
}
```


Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\build3[1].exe	JoeSecurity_Clipboard_Hijacker	Yara detected Clipboard Hijacker	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\build3[1].exe	Windows_Trojan_Clipbanker_f9f9e79d	unknown	unknown	• 0x1203:$a1: 7E 7E 0F B7 04 77 83 F8 41 74 69 83 F8 42 74 64 83 F8 43 74 5F 83
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\build3[1].exe	Windows_Trojan_Clipbanker_787b130b	unknown	unknown	• 0xefa:$mutex_setup: 55 8B EC 83 EC 18 53 56 57 E8 F8 F4 FF FF 68 30 30 40 00 6A 00 6A 00 FF 15 40 40 40 00 FF 15 2C 40 40 00 3D B7 00 00 00 75 08 6A 00 FF 15 10 30 40 00 • 0xf87:$new_line_check: 0F B7 C2 89 45 EC 0F B7 C2 83 F8 0A 74 43 BA 0D 0A 00 00 66 3B C2 74 39 83 F8 0D 74 34 83 F8 20 74 2F 83 F8 09 74 2A • 0xf87:$regex1: 0F B7 C2 89 45 EC 0F B7 C2 83 F8 0A 74 43 BA 0D 0A 00 00 66 3B C2 74 39 83 F8 0D 74 34 83 F8 20 74 2F 83 F8 09 74 2A • 0x12ad:$regex2: 6A 34 59 66 39 0E 75 7C 0F B7 46 02 6A 30 5A 83 F8 41 74 37 83 F8 42 74 32 66 3B C2 74 2D 83 F8 31 74 28 83 F8 32 74 23 83 F8 33 74 1E 66 3B C1 74 19 83 F8 35 74 14 83 F8 36 74 0F 83 F8 37 74 ... • 0x1335:$regex3: 56 8B F1 56 FF 15 20 40 40 00 83 F8 5F 0F 85 84 00 00 00 6A 38 59 66 39 0E 75 7C 0F B7 46 02 6A 30 5A 83 F8 41 74 37 83 F8 42 74 32 66 3B C2 74 2D 83 F8 31 74 28 83 F8 32 74 23 83 F8 33 74 1E ...
C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe	JoeSecurity_Clipboard_Hijacker	Yara detected Clipboard Hijacker	Joe Security	
C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe	Windows_Trojan_Clipbanker_f9f9e79d	unknown	unknown	• 0x1203:$a1: 7E 7E 0F B7 04 77 83 F8 41 74 69 83 F8 42 74 64 83 F8 43 74 5F 83

Click to see the 16 entries

Memory Dumps

Source	Rule	Description	Author	Strings
00000026.00000002.505614178.00000000007D0000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000026.00000002.505614178.00000000007D0000.00000004.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x644:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
00000000.00000002.380036043.0000000000859000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x721c:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000007.00000002.460164953.0000000000800000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000016.00000000.460937652.0000000000061000.00000020.00000001.01000000.00000011.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	

Click to see the 114 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
30.0.build3.exe.1000000.0.unpack	Windows_Trojan_Clipbanker_f9f9e79d	unknown	unknown	• 0x1203:$a1: 7E 7E 0F B7 04 77 83 F8 41 74 69 83 F8 42 74 64 83 F8 43 74 5F 83

Source	Rule	Description	Author	Strings
30.0.build3.exe.1000000.0.unpack	Windows_Trojan_Clipbanker_787b130b	unknown	unknown	• 0xefa:$mutex_setup: 55 8B EC 83 EC 18 53 56 57 E8 F8 F4 FF FF 68 30 30 00 01 6A 00 6A 00 FF 15 40 40 00 01 FF 15 2C 40 00 01 3D B7 00 00 00 75 08 6A 00 FF 15 10 30 00 01 • 0xf87:$new_line_check: 0F B7 C2 89 45 EC 0F B7 C2 83 F8 0A 74 43 BA 0D 0A 00 00 66 3B C2 74 39 83 F8 0D 74 34 83 F8 20 74 2F 83 F8 09 74 2A • 0xf87:$regex1: 0F B7 C2 89 45 EC 0F B7 C2 83 F8 0A 74 43 BA 0D 0A 00 00 66 3B C2 74 39 83 F8 0D 74 34 83 F8 20 74 2F 83 F8 09 74 2A • 0x12ad:$regex2: 6A 34 59 66 39 0E 75 7C 0F B7 46 02 6A 30 5A 83 F8 41 74 37 83 F8 42 74 32 66 3B C2 74 2D 83 F8 31 74 28 83 F8 32 74 23 83 F8 33 74 1E 66 3B C1 74 19 83 F8 35 74 14 83 F8 36 74 0F 83 F8 37 74 ... • 0x1335:$regex3: 56 8B F1 56 FF 15 20 40 00 01 83 F8 5F 0F 85 84 00 00 00 6A 38 59 66 39 0E 75 7C 0F B7 46 02 6A 30 5A 83 F8 41 74 37 83 F8 42 74 32 66 3B C2 74 2D 83 F8 31 74 28 83 F8 32 74 23 83 F8 33 74 1E ...
32.2.build2.exe.400000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
20.2.3C54.exe.408ef90.0.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
22.2.NewPlayer.exe.60000.0.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
Click to see the 128 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN DNS Query to SmokeLoader Domain (potunulit .org) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.857990532045695 05/28/23-10:42:32.589547
SID:	2045695
Source Port:	57990
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Blackmoon CnC Activity - Source IP: 192.168.2.3 - Destination IP: 103.100.211.218

Timestamp:	192.168.2.3103.100.211.21849720802839238 05/28/23-10:42:49.105133
SID:	2839238
Source Port:	49720
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN DNS Query to SmokeLoader Domain (potunulit .org) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.853975532045695 05/28/23-10:42:39.331614
SID:	2045695
Source Port:	53975
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/Filecoder.STOP Variant Public Key Download - Source IP: 211.59.14.90 - Destination IP: 192.168.2.3

Timestamp:	211.59.14.90192.168.2.380497142036335 05/28/23-10:42:46.297030
SID:	2036335
Source Port:	80

Destination Port:	49714
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/Vodkagats Loader Requesting Payload - Source IP: 192.168.2.3 - Destination IP: 123.140.161.243	
Timestamp:	192.168.2.3123.140.161.24349713802036333 05/28/23-10:42:45.165749
SID:	2036333
Source Port:	49713
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN DNS Query to SmokeLoader Domain (potunulit .org) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.860767532045695 05/28/23-10:42:51.638861
SID:	2045695
Source Port:	60767
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN DNS Query to SmokeLoader Domain (potunulit .org) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.859636532045695 05/28/23-10:42:45.594129
SID:	2045695
Source Port:	59636
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/Filecoder.STOP Variant Public Key Download - Source IP: 175.119.10.231 - Destination IP: 192.168.2.3	
Timestamp:	175.119.10.231192.168.2.380497112036335 05/28/23-10:42:45.790332
SID:	2036335
Source Port:	80
Destination Port:	49711
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Potential Dridex.Maldoc Minimal Executable Request - Source IP: 192.168.2.3 - Destination IP: 175.119.10.231	
Timestamp:	192.168.2.3175.119.10.23149721802020826 05/28/23-10:42:51.341437
SID:	2020826
Source Port:	49721
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Potential Dridex.Maldoc Minimal Executable Request - Source IP: 192.168.2.3 - Destination IP: 123.140.161.243	
Timestamp:	192.168.2.3123.140.161.24349713802020826 05/28/23-10:42:45.165749
SID:	2020826
Source Port:	49713
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN STOP Ransomware CnC Activity - Source IP: 192.168.2.3 - Destination IP: 211.59.14.90	
Timestamp:	192.168.2.3211.59.14.9049714802833438 05/28/23-10:42:45.438118
SID:	2833438
Source Port:	49714
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN DNS Query to SmokeLoader Domain (potunulit .org) - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.856924532045695 05/28/23-10:42:38.041315
SID:	2045695
Source Port:	56924
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/Vodkagats Loader Requesting Payload - Source IP: 192.168.2.3 - Destination IP: 175.119.10.231	
Timestamp:	192.168.2.3175.119.10.23149721802036333 05/28/23-10:42:51.341437
SID:	2036333
Source Port:	49721
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain
Antivirus detection for dropped file
Found malware configuration
Multi AV Scanner detection for submitted file
Multi AV Scanner detection for domain / URL
Multi AV Scanner detection for dropped file
Machine Learning detection for sample
Sample uses string decryption to hide its real strings
Machine Learning detection for dropped file

Compliance

Detected unpacking (overwrites its own PE header)

Networking

System process connects to network (likely due to code injection or exploit)
Snort IDS alert for network traffic
Uses known network protocols on non-standard ports
C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands

Found ransom note / readme
Yara detected Babuk Ransomware
Yara detected Djvu Ransomware
Modifies existing user documents (likely ransomware behavior)
Writes a notice file (html or txt) to demand a ransom

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Persistence and Installation Behavior

Yara detected Amadey bot

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Checks if the current machine is a virtual machine (disk enumeration)

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Benign windows process drops PE files

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected Amadeys stealer DLL

Yara detected SmokeLoader

Yara detected Amadey bot

Yara detected Clipboard Hijacker

Yara detected Fabookie

Yara detected Vidar stealer

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Crypto Currency Wallets

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Yara detected SmokeLoader

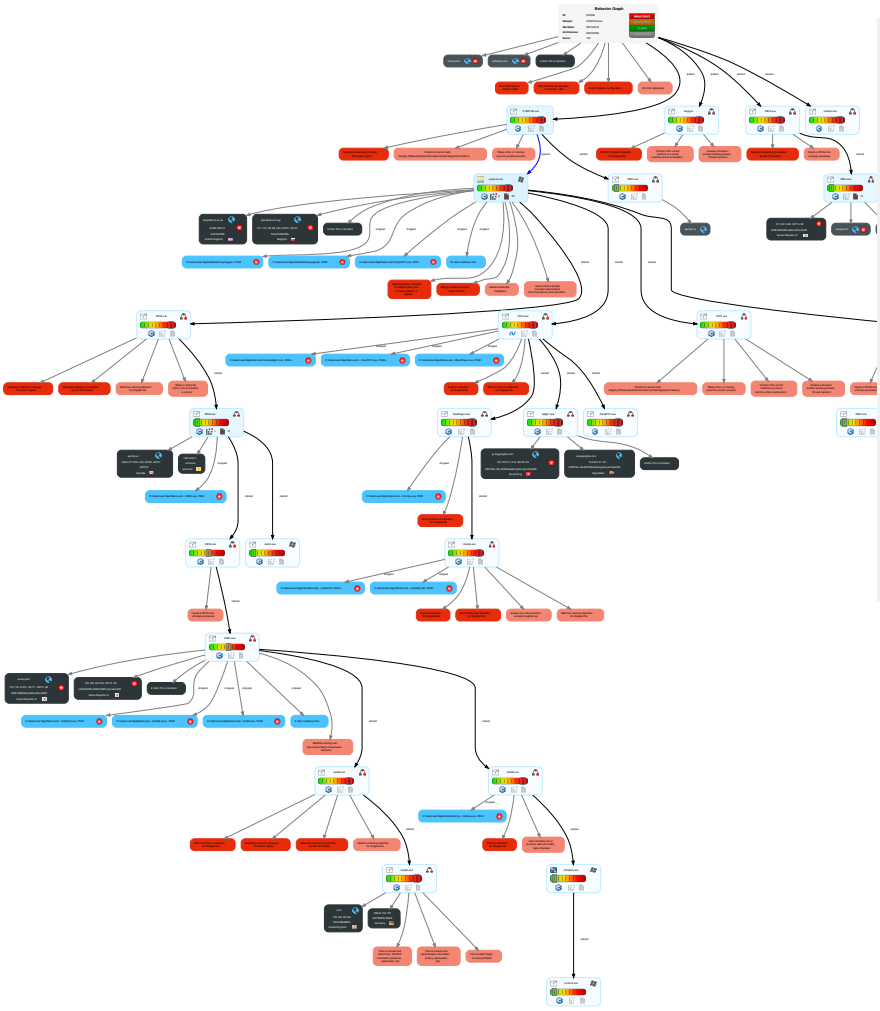
Yara detected Fabookie

Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 Scheduled Task/Job	4 1 2 Process Injection	1 Disable or Modify Tools	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	2 Data Encrypted for Impact
Default Accounts	1 Native API	1 1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 Deobfuscate/Decode Files or Information	1 Input Capture	3 File and Directory Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Exploitation for Client Execution	1 Services File Permissions Weakness	1 1 Registry Run Keys / Startup Folder	3 1 Obfuscated Files or Information	1 Credentials in Registry	4 5 System Information Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	1 1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 Command and Scripting Interpreter	Logon Script (Mac)	1 Services File Permissions Weakness	2 2 Software Packing	NTDS	1 Query Registry	Distributed Component Object Model	Input Capture	Scheduled Transfer	5 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	1 Scheduled Task/Job	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	4 4 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	1 2 6 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Masquerading	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 1 Virtualization/Sandbox Evasion	DCSync	1 3 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	4 1 2 Process Injection	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Services File Permissions Weakness	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

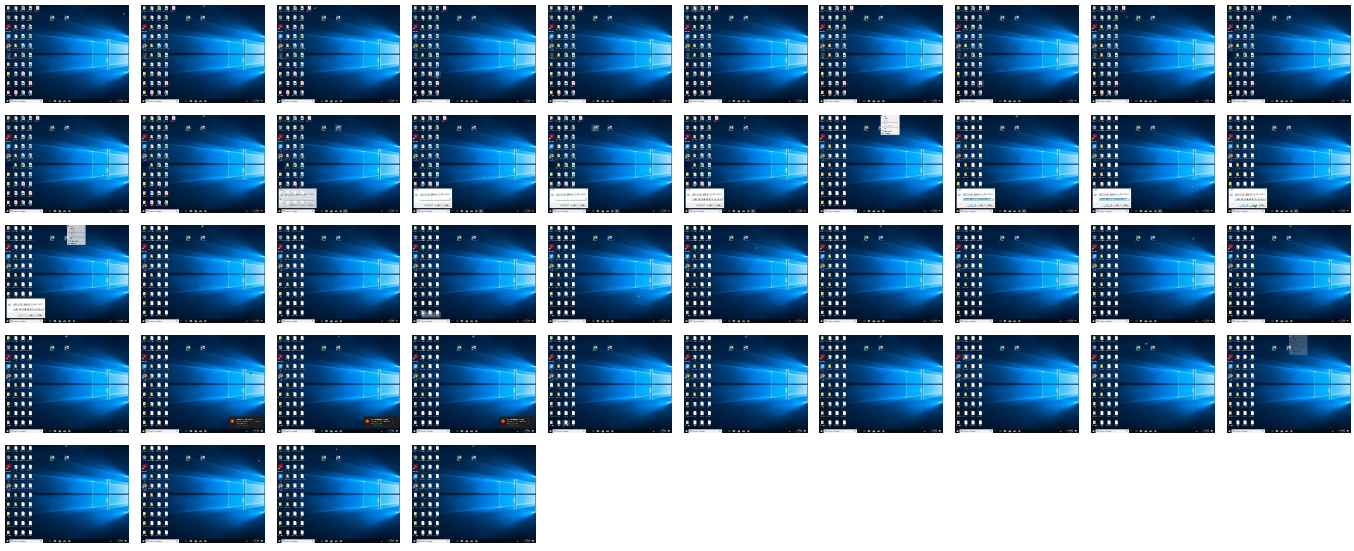
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
01860199.exe	38%	ReversingLabs		
01860199.exe	38%	Virustotal		Browse
01860199.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	100%	Avira	HEUR/AGEN.1301090	
C:\Users\user\AppData\Local\Temp\9F31.exe	100%	Avira	HEUR/AGEN.1357339	
C:\Users\user\AppData\Local\Temp\5DA0.exe	100%	Avira	HEUR/AGEN.1357339	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\build3[1].exe	100%	Avira	TR/Crypt.XPACK.Gen8	
C:\Users\user\AppData\Local\Temp\6FA9.exe	100%	Avira	HEUR/AGEN.1357339	
C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build3.exe	100%	Avira	TR/Crypt.XPACK.Gen8	
C:\Users\user\AppData\Local\Temp\3C54.exe	100%	Avira	HEUR/AGEN.1357339	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe	100%	Avira	HEUR/AGEN.1319380	
C:\Users\user\AppData\Local\Temp\D804.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\57DC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\9F31.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B46F.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\5DA0.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\A3D5.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\BC2.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\D689.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\EA44.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\388B.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\CBE6.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\build2[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\C861.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\673.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\A170.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\3E02.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6FA9.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B8C8.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\F4F7.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\3C54.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\913F.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe	87%	ReversingLabs	Win32.Trojan.Smokeloader	
C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build3.exe	88%	ReversingLabs	Win32.Trojan.ClipBanker	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\build2[1].exe	87%	ReversingLabs	Win32.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\build3[1].exe	88%	ReversingLabs	Win32.Trojan.ClipBanker	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	83%	ReversingLabs	Win64.Trojan.Amadey	
C:\Users\user\AppData\Local\Temp\3C54.exe	70%	ReversingLabs	ByteCode-MSIL.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\57DC.exe	43%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\5DA0.exe	70%	ReversingLabs	ByteCode-MSIL.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\6FA9.exe	70%	ReversingLabs	ByteCode-MSIL.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe	88%	ReversingLabs	Win32.Trojan.Privateloader	
C:\Users\user\AppData\Local\Temp\913F.exe	71%	ReversingLabs	Win32.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\9F31.exe	70%	ReversingLabs	ByteCode-MSIL.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\A170.exe	71%	ReversingLabs	Win32.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\A3D5.exe	71%	ReversingLabs	Win32.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\B8C8.exe	71%	ReversingLabs	Win32.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\D689.exe	71%	ReversingLabs	Win32.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\NewPlayer.exe	88%	ReversingLabs	Win32.Trojan.Privateloader	
C:\Users\user\AppData\Local\Temp\XandETC.exe	73%	ReversingLabs	Win64.Coinminer.Xmrig	
C:\Users\user\AppData\Local\Temp\aafg31.exe	33%	ReversingLabs	Win64.Trojan.Generic	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\07c6bc37dc5087\cred64.dll	83%	ReversingLabs	Win64.Trojan.Amadey	
C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe	88%	ReversingLabs	Win32.Trojan.ClipBanker	
C:\Users\user\AppData\Roaming\hwgujdv	38%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
toobussy.com	3%	Virustotal		Browse
colisumy.com	24%	Virustotal		Browse
potunulit.org	22%	Virustotal		Browse
jp.imgjeoighw.com	19%	Virustotal		Browse
speedlab.com.eg	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://potunulit.org/	0%	URL Reputation	safe	
http://jp.imgjeoighw.com/sts/image.jpg	0%	URL Reputation	safe	
http://ss.apjeoighw.com/	0%	URL Reputation	safe	
http://zexeq.com/raud/get.php	100%	URL Reputation	malware	
http://kingpirate.ru/tmp/	0%	URL Reputation	safe	
http://components.groove.net/Groove/Components/Root.osd?Package=net.groove.Groove.Tools.System.Groov	0%	URL Reputation	safe	
http://45.9.74.80/power.exe	100%	URL Reputation	malware	
http://components.groove.net/Groove/Components/SystemComponents/SystemComponents.osd?Package=net.gro	0%	URL Reputation	safe	
http://zexeq.com/files/1/build3.exe$run	100%	URL Reputation	malware	
http://ss.apjeoighw.com/check/safe	0%	URL Reputation	safe	
http://colisumy.com/dl/build2.exe	100%	URL Reputation	malware	
http://https://freebl3.dllmozglue.dllmsvcp140.dllnss3.dllsoftokn3.dllvcruntime140.dll	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://zexeq.com/files/1/build3.exe	0%	URL Reputation	safe	
http://zexeq.com/raud/get.php?pid=F4B58C92E14ED1DB6A495C4F0112806C&first=trueQ58	100%	Avira URL Cloud	malware	
http://https://we.tl/t-tnzomMj6	0%	Avira URL Cloud	safe	
http://ss.apjeoighw.com/check/safe3	0%	Avira URL Cloud	safe	
http://zexeq.com/files/1/build3.exel	100%	Avira URL Cloud	malware	
http://colisumy.com/dl/build2.exe$run	100%	Avira URL Cloud	malware	
45.9.74.80/0bjdn2Z/index.php	100%	Avira URL Cloud	malware	
http://colisumy.com/dl/build2.exerun3	100%	Avira URL Cloud	malware	
http://https://shsplatform.co.uk/tmp/index.php	100%	Avira URL Cloud	malware	
http://45.9.74.80/0bjdn2Z/Plugins/clip64.dll	100%	Avira URL Cloud	malware	
http://188.34.154.187:30303/addon.zip	0%	Avira URL Cloud	safe	
http://45.9.74.80/0bjdn2Z/Plugins/cred64.dll	100%	Avira URL Cloud	malware	
http://ss.apjeoighw.com/check/safe)	0%	Avira URL Cloud	safe	
http://194.180.48.90/cc.exe	0%	Avira URL Cloud	safe	
http://ss.apjeoighw.com:80/check/safe	0%	Avira URL Cloud	safe	
http://https://speedlab.com.eg/tmp/index.php	0%	Avira URL Cloud	safe	
http://ss.apjeoighw.com/check/safe1B	0%	Avira URL Cloud	safe	
http://zexeq.com/files/1/build3.exe$runZT	100%	Avira URL Cloud	malware	
http://toobussy.com/	0%	Avira URL Cloud	safe	
http://jp.imgjeoighw.com/sts/image.jpgO	100%	Avira URL Cloud	malware	
http://ss.apjeoighw.com/check/?sid=436160&key=a96ab7e5e6412d32675599dfaebc13f6	0%	Avira URL Cloud	safe	
http://zexeq.com/raud/get.phpep	100%	Avira URL Cloud	malware	
http://wuc11.com/tmp/	0%	Avira URL Cloud	safe	
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://ss.apjeoighw.com/blob:	0%	Avira URL Cloud	safe	
http://zexeq.com/raud/get.php?pid=F4B58C92E14ED1DB6A495C4F0112806C	100%	Avira URL Cloud	malware	
http://188.34.154.187:30303/	0%	Avira URL Cloud	safe	
http://ss.apjeoighw.com/check/?sid=436336&key=3f9d01718af2d5daf3c654f2052d5bc7	0%	Avira URL Cloud	safe	
http://45.9.74.80/0bjdn2Z/index.php	100%	Avira URL Cloud	malware	
http://zexeq.com/raud/get.php?pid=F4B58C92E14ED1DB6A495C4F011280Nkx%	100%	Avira URL Cloud	malware	
http://zexeq.com/raud/get.php?pid=F4B58C92E14ED1DB6A495C4F0112806C&first=true	100%	Avira URL Cloud	malware	
http://colisumy.com/dl/build.exe	100%	Avira URL Cloud	malware	
http://zexeq.com/files/1/build3.exe$runyinstall020921_delay721_sec.exe0	100%	Avira URL Cloud	malware	
http://188.34.154.187:30303/e44c96dfdf315ccf17cdd4b93cfe6e48	0%	Avira URL Cloud	safe	
http://ss.apjeoighw.com/check/?sid=436234&key=2cef0d99b721939135d08fea0dcaba52	0%	Avira URL Cloud	safe	
http://toobussy.com/tmp/	100%	Avira URL Cloud	malware	
http://ss.apjeoighw.com:80/check/?sid=436234&key=2cef0d99b721939135d08fea0dcaba52G_	0%	Avira URL Cloud	safe	
http://45.9.74.80/0bjdn2Z/index.php?scr=1	100%	Avira URL Cloud	malware	
http://ladogatur.ru/tmp/	0%	Avira URL Cloud	safe	
http://https://we.tl/t-tnzomMj6HU	0%	Avira URL Cloud	safe	
http://zexeq.com/raud/get.php?pid=F4B58C92E14ED1DB6A495C4F0112806Cg	100%	Avira URL Cloud	malware	
http://zexeq.com/files/1/build3.exerunb10	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
toobussy.com	222.236.49.123	true	true	• 3%, Virustotal, Browse	unknown
star-mini.c10r.facebook.com	157.240.9.35	true	false		high
star.c10r.facebook.com	157.240.17.17	true	false		high
colisumy.com	211.119.84.112	true	true	• 24%, Virustotal, Browse	unknown
potunulit.org	188.114.97.7	true	true	• 22%, Virustotal, Browse	unknown
jp.imgjeoighw.com	103.100.211.218	true	true	• 19%, Virustotal, Browse	unknown
speedlab.com.eg	217.174.148.28	true	true	• 1%, Virustotal, Browse	unknown
t.me	149.154.167.99	true	false		high
ss.apjeoighw.com	154.221.31.191	true	false		unknown
api.2ip.ua	162.0.217.254	true	false		high
shsplatform.co.uk	80.66.203.53	true	true		unknown
zexeq.com	175.119.10.231	true	true		unknown
www.facebook.com	unknown	unknown	false		high
adsmanager.facebook.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://potunulit.org/	true	• URL Reputation: safe	unknown
http://https://shsplatform.co.uk/tmp/index.php	true	• Avira URL Cloud: malware	unknown
http://jp.imgjeoighw.com/sts/image.jpg	true	• URL Reputation: safe	unknown
http://45.9.74.80/0bjdn2Z/Plugins/cred64.dll	true	• Avira URL Cloud: malware	unknown
http://zexeq.com/raud/get.php	true	• URL Reputation: malware	unknown
45.9.74.80/0bjdn2Z/index.php	true	• Avira URL Cloud: malware	low
http://https://steamcommunity.com/profiles/76561199508624021	false		high
http://188.34.154.187:30303/addon.zip	false	• Avira URL Cloud: safe	unknown
http://45.9.74.80/0bjdn2Z/Plugins/clip64.dll	true	• Avira URL Cloud: malware	unknown
http://kingpirate.ru/tmp/	true	• URL Reputation: safe	unknown
http://194.180.48.90/cc.exe	true	• Avira URL Cloud: safe	unknown
http://https://speedlab.com.eg/tmp/index.php	true	• Avira URL Cloud: safe	unknown
http://https://adsmanager.facebook.com/ads/manager/account_settings/account_billing/	false		high
http://45.9.74.80/power.exe	true	• URL Reputation: malware	unknown
http://https://t.me/looking_glassbot	false		high
http://ss.apjeoighw.com/check/?sid=436160&key=a96ab7e5e6412d32675599dfaebc13f6	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://wuc11.com/tmp/	true	• Avira URL Cloud: safe	unknown
http://zexeq.com/raud/get.php?pid=F4B58C92E14ED1DB6A495C4F0112806C	true	• Avira URL Cloud: malware	unknown
http://188.34.154.187:30303/	false	• Avira URL Cloud: safe	unknown
http://45.9.74.80/0bjdn2Z/index.php	true	• Avira URL Cloud: malware	unknown
http://ss.apjeoighw.com/check/?sid=436336&key=3f9d01718af2d5daf3c654f2052d5bc7	false	• Avira URL Cloud: safe	unknown
http://colisumy.com/dl/build.exe	true	• Avira URL Cloud: malware	unknown
http://zexeq.com/raud/get.php?pid=F4B58C92E14ED1DB6A495C4F0112806C&first=true	true	• Avira URL Cloud: malware	unknown
http://ss.apjeoighw.com/check/safe	false	• URL Reputation: safe	unknown
http://colisumy.com/dl/build2.exe	true	• URL Reputation: malware	unknown
http://https://api.2ip.ua/geo.json	false		high
http://188.34.154.187:30303/e44c96dfdf315ccf17cdd4b93cfe6e48	false	• Avira URL Cloud: safe	unknown
http://ss.apjeoighw.com/check/?sid=436234&key=2cef0d99b721939135d08fea0dcaba52	false	• Avira URL Cloud: safe	unknown
http://45.9.74.80/0bjdn2Z/index.php?scr=1	true	• Avira URL Cloud: malware	unknown
http://toobussy.com/tmp/	true	• Avira URL Cloud: malware	unknown
http://ladogatur.ru/tmp/	true	• Avira URL Cloud: safe	unknown
http://https://www.facebook.com/login.php?next=https%3A%2F%2Fadsmanager.facebook.com%2Fads%2Fmanager%2Faccount_settings%2Faccount_billing%2F	false		high
http://zexeq.com/files/1/build3.exe	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/y-/l/0	aafg31.exe, 00000015.00000003.535524540.000001E292293000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.644310592.000001E292380000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.616407141.000001E2922D0000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yt/r/v75M7CPu9-P.js?_nc_x=lj3Wp8lg5Kz	aafg31.exe, 00000015.00000003.616139527.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.617336652.000001E292381000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.558548528.000001E2922B9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.559523108.000001E29229C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593963921.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593189980.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E2922CB000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.560301255.000001E29229E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E292293000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://steamcommunity.com/profiles/76561199508624021update.zipopenopen_NULL%s	build2.exe, 00000018.00000002.478126519.0000000000840000.00000040.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://messenger.com/	aafg31.exe, 00000015.00000003.616407141.000001E2922BE000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.616139527.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.617336652.000001E292381000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.616875927.000001E2922D3000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.558548528.000001E2922B9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.559523108.000001E29229C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593963921.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593189980.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593189980.000001E2922BE000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.616407141.000001E2922D0000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://zexeq.com/files/1/build3.exel	D804.exe, 00000013.00000002.636070288.000000320F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/yL/r/camCPYrr6r7.js?_nc_x=lj3Wp8lg5Kz	aafg31.exe, 00000015.00000003.616407141.000001E2922BE000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.617256768.000001E292290000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.616139527.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.536338668.000001E292285000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.616875927.000001E2922D3000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.558548528.000001E2922B9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593963921.000001E2922D6000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.559523108.000001E29229C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593963921.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.536309898.000001E292289000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593189980.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593189980.000001E2922BE000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E2922CB000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.558924559.000001E292285000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.617144495.000001E292287000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.560301255.000001E29229E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E292293000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.644310592.000001E292380000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.616407141.000001E2922D0000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://colisumy.com/dl/build2.exe$run	D804.exe, 00000013.00000002.619178225.000000006AF000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ss.apjeoighw.com/	aafg31.exe, 00000015.00000002.618777053.000001E291A70000.00000004.00001000.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.632373221.000001E291FA0000.00000040.00001000.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.635269175.000001E292110000.00000040.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://colisumy.com/dl/build2.exerun3	D804.exe, 00000013.00000002.619178225.000000062B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://t.me/looking_glassbotlookataddon.zipMozilla/5.0	build2.exe, 00000018.00000002.478126519.0000000000840000.00000040.00001000.00020000.00000000.sdmp	false		high
http://https://we.tl/t-tnzomMj6	D804.exe, 00000013.00000002.619178225.000000006BB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	D804.exe, 00000013.00000003.475323189.000000032B0000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.jsonyY&$	D804.exe, 00000010.00000002.619429561.000000000808000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/u	D804.exe, 00000013.00000003.452681314.000000000647000.00000004.00000020.00020000.00000000.sdmp, D804.exe, 00000013.00000002.619178225.000000000062B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ss.apjeoighw.com/check/safe3	aafg31.exe, 00000015.00000002.642437211.000001E292275000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://zexeq.com/raud/get.php?pid=F4B58C92E14ED1DB6A495C4F0112806C&first=trueQ58	D804.exe, 00000013.00000002.619178225.000000006AF000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/y2/l/0	aafg31.exe, 00000015.00000003.616139527.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.617336652.000001E292381000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.558548528.000001E2922B9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.559523108.000001E29229C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593963921.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593189980.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E2922CB000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.560301255.000001E29229E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E292293000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.jsonV	D804.exe, 00000013.00000002.619178225.000000005F7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yP/l/0	aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://components.groove.net/Groove/Components/Root.osd?Package=net.groove.Groove.Tools.System.Groov	explorer.exe, 00000001.00000000.378821866.00007FFC1B439000.00000002.00000001.01000000.00000005.sdmp	false	• URL Reputation: safe	unknown
http://ss.apjeoighw.com/check/safe)	aafg31.exe, 00000015.00000002.642437211.000001E292275000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ss.apjeoighw.com:80/check/safe	aafg31.exe, 00000015.00000003.539647639.000001E2901A6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/yO/r/_tJ17sGyxOX.js?_nc_x=Ij3Wp8lg5Kz	aafg31.exe, 00000015.00000003.559161122.000001E2901D6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ss.apjeoighw.com/check/safe1B	aafg31.exe, 00000015.00000002.618169870.000001E2900FB000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.2ip.ua/geo.jsonG.S	D804.exe, 00000006.00000002.450438133.000000000707000.00000004.00000020.00020000.00000000.sdmp	false		high
http://zexeq.com/files/1/build3.exe$runZT	D804.exe, 00000013.00000002.619178225.000000000680000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://zexeq.com/raud/get.phpep	D804.exe, 00000010.00000002.619429561.000000000808000.00000004.00000020.00020000.00000000.sdmp, D804.exe, 00000013.00000002.619178225.0000000000680000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://api.2ip.ua/?	D804.exe, 00000013.00000003.452681314.000000000647000.00000004.00000020.00020000.00000000.sdmp, D804.exe, 00000013.00000002.619178225.000000000062B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.youtube.com/	D804.exe, 00000013.00000003.475594980.000000032B0000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.json1	A170.exe, 0000001D.00000002.490407985.000000008D7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yB/l/0	aafg31.exe, 00000015.00000003.616139527.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.617336652.000001E292381000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.558548528.000001E2922B9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.559523108.000001E29229C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593963921.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593189980.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E2922CB000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.560301255.000001E29229E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E292293000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://jp.imgjeoighw.com/sts/image.jpgO	aafg31.exe, 00000015.00000002.618169870.000001E2900FB000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/yI/r/Ib90vcVxYzI.js?_nc_x=Ij3Wp8lg5Kz	aafg31.exe, 00000015.00000003.559161122.000001E2901D6000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.617144495.000001E292287000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.643446636.000001E29228C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://toobussy.com/	aafg31.exe, 00000015.00000003.616407141.000001E2922EB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://api.2ip.ua/geo.jsonA	A170.exe, 0000001D.00000002.490407985.000000008D7000.00000004.00000020.00020000.00000000.sdmp	false		high

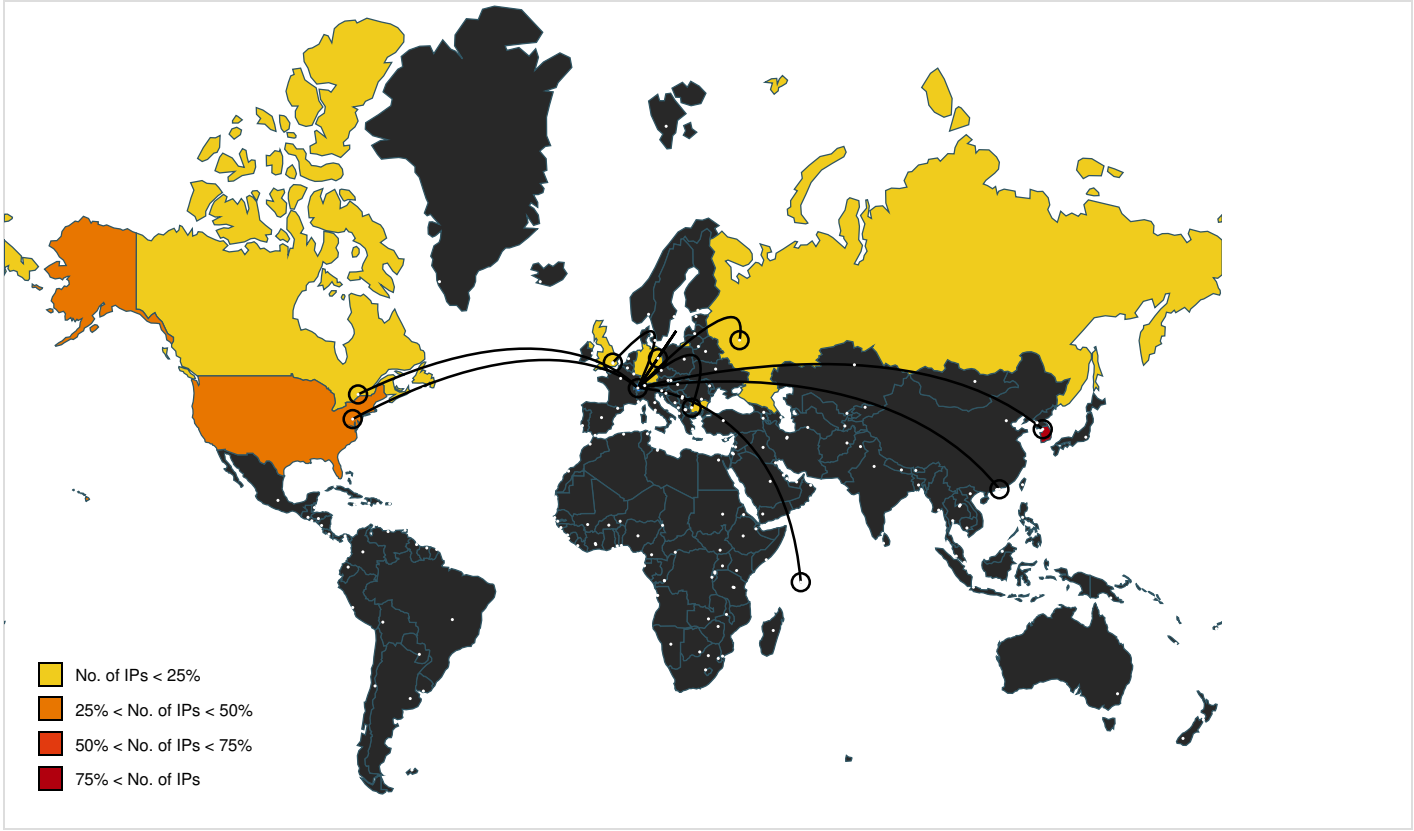
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/yK/l/0	aafg31.exe, 00000015.00000003.535524540.000001E292293000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.644310592.000001E292380000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.616407141.000001E2922D0000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yn/r/A-4As8UDAZ8.js?_nc_x=lj3Wp8lg5Kz	aafg31.exe, 00000015.00000003.616139527.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.617336652.000001E292381000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.558548528.000001E2922B9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.559523108.000001E29229C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593963921.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593189980.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E2922CB000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.560301255.000001E29229E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E292293000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/y4/r/ZZnKfYusN8Z.js?_nc_x=lj3Wp8lg5Kz	aafg31.exe, 00000015.00000003.616139527.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.617336652.000001E292381000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.558548528.000001E2922B9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.559523108.000001E29229C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593963921.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593189980.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E2922CB000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.560301255.000001E29229E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E292293000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://components.groove.net/Groove/Components/SystemComponents/SystemComponents.osd?Package=net.gro	explorer.exe, 00000001.00000000.37882186.00007FFC1B439000.00000002.00000001.01000000.00000005.sdmp	false	• URL Reputation: safe	unknown
http://www.amazon.com/	D804.exe, 00000013.00000003.474950384.000000032B0000.00000004.00001000.00020000.00000000.sdmp	false		high
http://zexeq.com/files/1/build3.exe$run	D804.exe, 00000013.00000002.619178225.00000000680000.00000004.00000020.00020000.00000000.sdmp, D804.exe, 00000013.00000002.619178225.00000000006AF000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://www.twitter.com/	D804.exe, 00000013.00000003.475504479.000000032B0000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.openssl.org/support/faq.html	D804.exe, 0000001C.00000002.491035809.000000002460000.00000040.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	D804.exe, 00000005.00000002.442867169.000000002690000.00000040.00001000.00020000.00000000.sdmp, D804.exe, 00000006.00000002.449975040.0000000000400000.00000040.00000400.00020000.00000000.sdmp, D804.exe, 0000000D.00000002.450667818.00000000025300000.00000040.00001000.00020000.00000000.sdmp, D804.exe, 00000010.00000002.617846506.0000000000400000.00000040.00000400.00020000.00000000.sdmp, D804.exe, 00000012.00000002.451684545.00000000024D0000.00000040.00001000.00020000.00000000.sdmp, D804.exe, 00000013.00000002.617779609.0000000000400000.00000040.00000400.00020000.00000000.sdmp, B46F.exe, 00000019.00000002.474131384.00000000024D0000.00000040.00001000.00020000.00000000.sdmp, B46F.exe, 0000001A.00000002.488867120.0000000000400000.00000040.00000400.00020000.00000000.sdmp, A170.exe, 0000001B.00000002.493740298.000000000024C0000.00000040.00001000.00020000.00000000.sdmp, D804.exe, 0000001C.00000002.491035809.0000000002460000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://static.xx.fbcdn.net/rsrc.php/v3/yT/r/Kp9IMjEGN_T.js?_nc_x=lj3Wp8lg5Kz	aafg31.exe, 00000015.00000003.616139527.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.617336652.000001E292381000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.558548528.000001E2922B9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.559523108.000001E29229C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593963921.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593189980.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E2922CB000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.560301255.000001E29229E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E292293000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yE/r/yWg6mkUCjYR.js?_nc_x=lj3Wp8lg5Kz	aafg31.exe, 00000015.00000003.616139527.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.617336652.000001E292381000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.558548528.000001E2922B9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.559523108.000001E29229C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593963921.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593189980.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E2922CB000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.560301255.000001E29229E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E292293000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ss.apjeoighw.com/blob:	aafg31.exe, 00000015.00000003.539122814.000001E2901D6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.2ip.ua/geo.jsonq	D804.exe, 00000013.00000003.452681314.000000000647000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.2ip.ua/geo.jsons	913F.exe, 00000025.00000002.514716181.000000000667000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yq/l/0	aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.644310592.000001E292380000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.616407141.000001E2922D0000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://zexeq.com/files/1/build3.exe$runyinstall020921_delay721_sec.exe0	D804.exe, 00000013.00000002.619178225.000000006AF000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://zexeq.com/raud/get.php?pid=F4B58C92E14ED1DB6A495C4F011280Nkx%	D804.exe, 00000010.00000002.619429561.000000000891000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.nytimes.com/	D804.exe, 00000013.00000003.475283762.000000032B0000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yE/l/0	aafg31.exe, 00000015.00000003.535524540.000001E292293000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.644310592.000001E292380000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.616407141.000001E2922D0000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/	B46F.exe, 0000001A.00000002.489404633.000000000687000.00000004.00000020.00020000.00000000.sdmp, A170.exe, 0000001D.00000003.488086932.0000000000939000.00000004.00000020.00020000.00000000.sdmp, A170.exe, 0000001D.00000002.490407985.000000000939000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t.me/looking_glassboeL	build2.exe, 00000018.00000002.478487593.00000000008C8000.00000040.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yO/r/_tJ17sGyx	aafg31.exe, 00000015.00000003.617144495.000001E292287000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.643446636.000001E29228C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.json#&	D804.exe, 00000010.00000003.452471512.000000000851000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://freebl3.dllmozglue.dllmsvcp140.dllnss3.dllsoftokn3.dllvcruntime140.dll	build2.exe, 00000018.00000002.478126519.0000000000840000.00000040.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ss.apjeoighw.com:80/check/?sid=436234&key=2cef0d99b721939135d08fea0dcaba52G_	aafg31.exe, 00000015.00000003.569051255.000001E2901A6000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.566066441.000001E2901A6000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.563228419.000001E2901A6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/ye/r/sczXDyPA0UL.js?_nc_x=lj3Wp8lg5Kz	aafg31.exe, 00000015.00000003.616139527.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.617336652.000001E292381000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.558548528.000001E2922B9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.559523108.000001E29229C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593963921.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593189980.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E2922CB000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.560301255.000001E29229E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E292293000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.wikipedia.com/	D804.exe, 00000013.00000003.475541394.000000032B0000.00000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://we.tl/t-tnzomMj6HU	D804.exe, 00000010.00000002.619429561.000000000891000.00000004.00000020.00020000.00000000.sdmp, D804.exe, 00000013.00000002.636070288.00000000031DB000.00000004.00000020.00020000.00000000.sdmp, D804.exe, 00000013.00000002.619178225.000000000680000.00000004.00000020.00020000.00000000.sdmp, D804.exe, 00000013.00000002.619178225.00000000006AF000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3i7M54/yx/l/en_US/LsRZeEzcd6B.js?_nc_x=lj3Wp8lg5Kz	aafg31.exe, 00000015.00000003.616139527.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.617336652.000001E292381000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.558548528.000001E2922B9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.559523108.000001E29229C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593963921.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.593189980.000001E2922F9000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E2922CB000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.560301255.000001E29229E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.535524540.000001E292293000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.595112195.000001E2922FA000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.592730628.000001E292381000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.live.com/	D804.exe, 00000013.00000003.475244622.000000032B0000.00000004.00001000.00020000.00000000.sdmp	false		high
http://zexeq.com/files/1/build3.exerunb10	D804.exe, 00000013.00000002.619178225.0000000062B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://zexeq.com/raud/get.php?pid=F4B58C92E14ED1DB6A495C4F0112806Cg	D804.exe, 00000010.00000002.619429561.000000000852000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.240.9.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
103.100.211.218	jp.imgjeoighw.com	Hong Kong		133115	HKKFGL-AS-APHKKwaifongGroupLimitedHK	true
154.221.31.191	ss.apjeoighw.com	Seychelles		133115	HKKFGL-AS-APHKKwaifongGroupLimitedHK	false
149.154.167.99	t.me	United Kingdom		62041	TELEGRAMRU	false
217.174.148.28	speedlab.com.eg	Bulgaria		31083	TELEPOINTBG	true
175.119.10.231	zexeq.com	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
211.40.39.251	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
157.240.17.17	star.c10r.facebook.com	United States		32934	FACEBOOKUS	false
211.119.84.112	colisumy.com	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
162.0.217.254	api.2ip.ua	Canada		35893	ACPCA	false
194.180.48.90	unknown	Germany		10753	LVLT-10753US	true
123.140.161.243	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
80.66.203.53	shsplatform.co.uk	United Kingdom		61323	UKFASTGB	true
188.34.154.187	unknown	Germany		24940	HETZNER-ASDE	false
45.9.74.80	unknown	Russian Federation		200740	FIRST-SERVER-EU-ASRU	true
211.59.14.90	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
188.114.97.7	potunulit.org	European Union		13335	CLOUDFLARENETUS	true
188.114.96.7	unknown	European Union		13335	CLOUDFLARENETUS	true
183.100.39.157	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
157.240.234.35	unknown	United States		32934	FACEBOOKUS	false
222.236.49.123	toobussy.com	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
222.236.49.124	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876998
Start date and time:	2023-05-28 10:41:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	43
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	01860199.exe
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.winEXE@76/330@105/23
EGA Information:	Failed
HDC Information:	• Successful, ratio: 45.2% (good quality ratio 38.6%) • Quality average: 61.8% • Quality standard deviation: 35.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, Conhost.exe, dllhost.exe, consent.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.89.179.12, 20.189.173.22, 20.42.73.29, 20.189.173.21
- Excluded domains from analysis (whitelisted): login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, onedsblobprdwus17.westus.cloudapp.azure.com, onedsblobprdwus16.westus.cloudapp.azure.com, watson.telemetry.microsoft.com, onedsblobprdcus17.centralus.cloudapp.azure.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:42:01	API Interceptor	556x Sleep call for process: explorer.exe modified
10:42:34	Task Scheduler	Run new task: Firefox Default Browser Agent 1D1CF5D964ED7B3F path: C:\Users\user\AppData\Roaming\hwgujdv
10:42:40	Task Scheduler	Run new task: Time Trigger Task path: C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe s>--Task
10:42:43	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe" --AutoStart
10:42:45	API Interceptor	1x Sleep call for process: D804.exe modified
10:42:46	API Interceptor	1x Sleep call for process: WerFault.exe modified
10:42:53	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe" --AutoStart
10:42:55	Task Scheduler	Run new task: Azure-Update-Task path: C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe
10:42:58	Task Scheduler	Run new task: mnolyk.exe path: C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe
10:42:59	API Interceptor	571x Sleep call for process: mnolyk.exe modified
10:43:09	API Interceptor	1x Sleep call for process: build2.exe modified
10:43:20	Task Scheduler	Run new task: Firefox Default Browser Agent A259CA271F5868C4 path: C:\Users\user\AppData\Roaming\ewgujdv
10:43:34	API Interceptor	1x Sleep call for process: aafg31.exe modified
10:43:50	Task Scheduler	Run new task: NoteUpdateTaskMachineQC path: C:\Program Files\Notepad\Chrome\updater.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\025625674549205065342453 98

Process:	C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 7, database pages 36, 1st free page 10, free pages 1, cookie 0x29, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	147456
Entropy (8bit):	0.7217007190866341
Encrypted:	false
SSDEEP:	384:kab+d5neKTnuRpHDiEwABBE3umab+QuJdi:kab+dVeK8iEZBBjmab+QuJdi
MD5:	FEF7F4B210100663DC7731400BAC534E
SHA1:	E3F17C46A2DB6861F22B3F4222B97DCB5EBBD47A
SHA-256:	E81118F5C967EA342A16BDEFB28919F8039E772F8BDCF4A65684E3F56D31EA0E

SHA-512:	6134CC2118FBADD137C4FC3204028B088C7E73A7B985A64D84C60ABD5B1DBFD0AA352C6DF199F43164FEC92378571B5FAC4F801E9AF7BE1DEA8FB6C3C799F 95
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....).....[5..... ....

C:\ProgramData\246938793374694400987379525

Process:	C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\ProgramData\39571994840354560723794613

Process:	C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 17, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 17
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.4755077381471955
Encrypted:	false
SSDEEP:	96:oesz0Rwhba5DX1tHQOd0AS4mcAMmgAU7MxTWbKSS:o+RwE55tHQOKB4mcmgAU7MxTWbNS
MD5:	DEE86123FE48584BA0CE07793E703560
SHA1:	E80D87A2E55A95BC937AC24525E51AE39D635EF7
SHA-256:	60DB12643ECF5B13E6F05E0FBC7E0453D073E0929412E39428D431DB715122C8
SHA-512:	65649B808C7AB01A65D18BF259BF98A4E395B091D17E49849573275B7B93238C3C9D1E5592B340ABCE3195F183943CA8FB18C1C6C2B5974B04FE99FCCF582BF
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

C:\ProgramData\61788534741070885639801227

Process:	C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CB F
Malicious:	false

Reputation:	unknown
Preview:	SQLite format 3.....@ .....[5..... ....

C:\ProgramData\689335643461943721122520 72

Process:	C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\ProgramData\952392497598068978748065 64

Process:	C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 7, database pages 36, 1st free page 10, free pages 1, cookie 0x29, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	147456
Entropy (8bit):	0.7217007190866341
Encrypted:	false
SSDEEP:	384:kab+d5neKTnuRpHDiEwABBE3umab+QuJdi:kab+dVeK8iEZBBjmab+QuJdi
MD5:	FEF7F4B210100663DC7731400BAC534E
SHA1:	E3F17C46A2DB6861F22B3F4222B97DCB5EBBD47A
SHA-256:	E81118F5C967EA342A16BDEFB28919F8039E772F8BDCF4A65684E3F56D31EA0E
SHA-512:	6134CC2118FBADD137C4FC3204028B088C7E73A7B985A64D84C60ABD5B1DBFD0AA352C6DF199F43164FEC92378571B5FAC4F801E9AF7BE1DEA8FB6C3C799F 95
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....).....[5..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_C861.exe_ee73edd8fcc59e6e41b76bbadce78e8978345d94_81c5b0e7_15a e9ed9\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8205242041362858
Encrypted:	false
SSDEEP:	96:eJxorFzUelJoWKixCto07RP6tpXIQcQjc6ieAcElcw3K+HbHg/8BRTf3o8Fa9iVi:1ZUeliWKGHtGZvPjIg/u7sXS274ItL
MD5:	630663FB4548437CAB9B71A117392776
SHA1:	428A1A4ED05F4C140B589DE9E5CE379E77A23A44
SHA-256:	35B2CB67E341CE0D02B479C13C3822EACA1BF1ABE1174D1807E0DB09B4E7EDAC
SHA-512:	5FD2F30697D0CC13887EBF452770A2FCB7AD761F61D4786F9509F932EE1ECD7EF146C4954C55D75ACC2D29BA11CCFEC03416B88AD861C5183E1CA104AE50C B1
Malicious:	false
Reputation:	unknown

Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.2.9.7.6.9.3.5.9.9.6.3.5.0.9.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.9.7.6.9.3.6.0.8.0.7.2.6.2.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.d.8.3.7.3.3.b.-.a.2.b.6.-.4.f.8.b.-.a.4.a.c.-.f.9.4.3.a.4.c.d.6.e.c.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.4.9.4.b.5.0.f.-.4.6.b.a.-.4.a.a.1.-.a.7.7.5.-.3.0.a.a.7.c.6.0.2.f.3.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.C.8.6.1...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.0.0.4.4.-.0.0.0.1.-.0.0.1.f.-.3.1.0.f.-.c.0.c.b.8.b.9.1.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.e.a.c.b.e.e.1.8.2.b.3.e.b.b.4.c.3.e.8.b.b.8.c.2.b.a.d.d.e.1.1.1.0.0.0.0.f.b.0.2.!.0.0.0.0.2.d.f.f.9.4.4.f.9.7.0.f.a.e.f.5.c.6.f.a.9.2.a.c.8.f.b.e.8.2.c.9.2.5.1.5.5.3.f.3.!.C.8.6.1...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.3././.0.3././.1.3.:.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sun May 28 17:42:40 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	34732
Entropy (8bit):	2.0489643020598747
Encrypted:	false
SSDEEP:	96:5V8J288/BlctnoyfBi7eJEnus9DBBLMv58iS3VzwexaeTrvMM4egPe+WI3+IX4IU:4JSUeyfBOeJ+iS3VzrbPMMBgWGJo+9o
MD5:	822CAB26CD9F624557FCEAC2B8A54E2A
SHA1:	D9F3FE71FBE434A0E63FC8AA29250153734802A2
SHA-256:	EA4C92CF376F45CE205D0B8C07B2084BD4AEF2B38C7A88A131698A979283873C
SHA-512:	68C9EC7024CD3AF6027A3FB05F309F814E32134FC7B8C6B297B4A997662104AAF8E9DEF588FFA7C5B5954EC6A9F685F15685BC5AE54AC588268D04C92486450
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....sd.....&.....T.....8.....T.....r.....U.....B.....8.....GenuineIntelW.....T.....D.....sd..... .....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8364
Entropy (8bit):	3.6992724605112297
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiTT69J6YqGHSUe7gmf9SRpqvCpDp89bKOsfo4um:RrlsNiH6j6Y1HSUagmf9SUKNfV
MD5:	F4E456151E22006370DF54340A9AB031
SHA1:	ECDC4E02D11843A25C6E40506E82B5DF7EE049A5
SHA-256:	CF0CBCC87429765C81C0B8E4CE5E321003576320A3F66EFAE699D7FA8155AADC
SHA-512:	13ED0EE28704FF51F7364AFDBB21C56D8C278768539A98AA757B1C200AC2CDA8C7517132F9136361737D52B83BCFD78B8A4709409D7EE83DBE745C3A648309C
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.<./.P.i.d.>.....<.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER86DE.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4680
Entropy (8bit):	4.4629285853594665
Encrypted:	false
SSDEEP:	48:cvIwSD8zs2JgtWI9fjWyWgc8sqYjH8fm8M4JNRjFgs+q8voR7gTEId:uITfM8ygrsqYQJKsKogTEId
MD5:	A30F7BD601F458CEAB46FD69CF16B469
SHA1:	5120BA2BCC141226ECAAA855EA4789F4475DC7EC
SHA-256:	7F6EC29D4DCBC81D6ED5059B848E6A69268700196CDD23DE757FF3D7BA56ECDA
SHA-512:	AF5DA4DB2C59C502BAC264465CD2BD09CA370AAB4E8253F58FCA5C1C1AB80D54FCFCF1F551AF0B1B41C4E8CB01820223AFA1BC3B7A74AD82835057A8EEF8B79
Malicious:	false
Reputation:	unknown

Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="2060813" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\SystemID\PersonalID.txt

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.993391529870108
Encrypted:	false
SSDEEP:	3:2dqkaPvGoFy:2KvG
MD5:	CAF15C2C1DBEB4F0A6E187F80F2BD109
SHA1:	461C5511D8DA0C60D8A0E749789D322D376580B4
SHA-256:	4C37EA89D270FBA2A8EE9CDE1C21CF690DCAAE2E717DD20BC6427DFCFE6234DD
SHA-512:	AEA59BCE0C2016E99CA20A2BBE5CD50BB9A0D9C9F336587084DF1B03520FA299EB8CEEAB9D4C8858CA636C25443464EAF70CFE7B81EAC9778AD29B21B889C EBD
Malicious:	false
Reputation:	unknown
Preview:	az8OAYewNgELvwQrvCQFNi4j455hRwuI26KpqTgc..

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	modified
Size (bytes):	623
Entropy (8bit):	7.672341084038176
Encrypted:	false
SSDEEP:	12:cbTqi+zWsjHDRwNRYrQ1QdEY2iZB5i55NTtlAREVFZjFtPixHfzGEGJcii9a:WTqi0WoRw7H1QWY2iFi53TOTbYHyECbD
MD5:	82E2E3ACA6EC2416013473A6F9BA61B3
SHA1:	EDEBF86B5B21E938F7B27821893AD52287A056EE
SHA-256:	767E13A8A8D96090DCA740ED213EFF855A9551F1805DF52676EE490E3E38222E
SHA-512:	9EECD1FD4EFB3B6BD5B0D56DB9F4B956A87126B61386224B205037339F686B25E0BD6B44E0668E624A63EEB65442E284B221891FEA46C601EFEF729CEBDDC6F5
Malicious:	false
Reputation:	unknown
Preview:	2020/.e.V....v...f.....VVm.}.C.tr.g.M.D.LR2........a.:.....~...*.....B.#...z;.F...'u.....>2/.f...........5.3@.5#..J..}...M. ..{.....N..t...<..&].'.h...uk=.l....(..9..~..7+..... c...NIH..cd..e$......:Y ..%.^#.....p...~...[.]....0.I..Z.s...2...#.qe.J.....:.i\.....+....);5..q.#..L[*...Zu.t..})......d..k.....u`.].gc?..l.?....{G..+|.D..,.m0.....&..[\...3?...M...;.${./.o...@..A.r..Y.C...Ex.=.K..?.!r....{.`....M)..X)..(si<...q'.|....x.>.bL..?u......>.y..[LY6..m.q....!.m{U..Ed....4U40j...pS..$..3..K.L!..R..c.az8OAYewNgELvwQrvCQFNi4j455hRwuI26KpqTgc{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	623
Entropy (8bit):	7.672341084038176
Encrypted:	false
SSDEEP:	12:cbTqi+zWsjHDRwNRYrQ1QdEY2iZB5i55NTtlAREVFZjFtPixHfzGEGJcii9a:WTqi0WoRw7H1QWY2iFi53TOTbYHyECbD
MD5:	82E2E3ACA6EC2416013473A6F9BA61B3
SHA1:	EDEBF86B5B21E938F7B27821893AD52287A056EE
SHA-256:	767E13A8A8D96090DCA740ED213EFF855A9551F1805DF52676EE490E3E38222E
SHA-512:	9EECD1FD4EFB3B6BD5B0D56DB9F4B956A87126B61386224B205037339F686B25E0BD6B44E0668E624A63EEB65442E284B221891FEA46C601EFEF729CEBDDC6F5
Malicious:	false
Reputation:	unknown
Preview:	2020/.e.V....v...f.....VVm.}.C.tr.g.M.D.LR2........a.:.....~...*.....B.#...z;.F...'u.....>2/.f...........5.3@.5#..J..}...M. ..{.....N..t...<..&].'.h...uk=.l....(..9..~..7+..... c...NIH..cd..e$......:Y ..%.^#.....p...~...[.]....0.I..Z.s...2...#.qe.J.....:.i\.....+....);5..q.#..L[*...Zu.t..})......d..k.....u`.].gc?..l.?....{G..+|.D..,.m0.....&..[\...3?...M...;.${./.o...@..A.r..Y.C...Ex.=.K..?.!r....{.`....M)..X)..(si<...q'.|....x.>.bL..?u......>.y..[LY6..m.q....!.m{U..Ed....4U40j...pS..$..3..K.L!..R..c.az8OAYewNgELvwQrvCQFNi4j455hRwuI26KpqTgc{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\2EM0SFDW\www.msn[1].xml	
Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	347
Entropy (8bit):	7.319964250408128
Encrypted:	false
SSDEEP:	6:QFHOvH6Q7kO+2ynIhsrj5MUGj3BrbTIUgSBRCn7lbzf6vLcii96Z:QIvHX7VQns45MNPENYRCn7lbzfGcii9a
MD5:	2F19EB9F2E99DF11E1754AD42CDCC60F
SHA1:	A1D17DBB19DFBA52F9E034759847808E494D6592
SHA-256:	8A48D0180CC204273FB8307BD0E26BD9AD27FE1C4FF4250F94F48132EC9F8A67
SHA-512:	71D2AFAC40AE7D0FCFA7E32A0555DB565D79979C400047BB6E53D0CB9F55DAB8F9D472B70834B27FB624B950A87658B263D924447488189A8F2C6A467120E314
Malicious:	false
Reputation:	unknown
Preview:	<root..T..7.....J..]..n0...5.#.....i...+b..qZ.c`!O....s...,$I...5h...."...z..n"40o...9....\&.\.k....M)..H.H..s.*.J2.....o.....d>..\..C@.q~....he....(.]....`Y.c..4.s..d.d]_tk....N.....^..B...N..l. .2.H..4..+..1B..58.)....2g..O..6....w..e...*..{..az8OAYewNgELvwQrvCQFNi4j455hRwuI26KpqTgc{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\2EM0SFDW\www.msn[1].xml.vapo (copy)	
Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	347
Entropy (8bit):	7.319964250408128
Encrypted:	false
SSDEEP:	6:QFHOvH6Q7kO+2ynIhsrj5MUGj3BrbTIUgSBRCn7lbzf6vLcii96Z:QIvHX7VQns45MNPENYRCn7lbzfGcii9a
MD5:	2F19EB9F2E99DF11E1754AD42CDCC60F
SHA1:	A1D17DBB19DFBA52F9E034759847808E494D6592
SHA-256:	8A48D0180CC204273FB8307BD0E26BD9AD27FE1C4FF4250F94F48132EC9F8A67
SHA-512:	71D2AFAC40AE7D0FCFA7E32A0555DB565D79979C400047BB6E53D0CB9F55DAB8F9D472B70834B27FB624B950A87658B263D924447488189A8F2C6A467120E314
Malicious:	false
Reputation:	unknown
Preview:	<root..T..7.....J..]..n0...5.#.....i...+b..qZ.c`!O....s...,$I...5h...."...z..n"40o...9....\&.\.k....M)..H.H..s.*.J2.....o.....d>..\..C@.q~....he....(.]....`Y.c..4.s..d.d]_tk....N.....^..B...N..l. .2.H..4..+..1B..58.)....2g..O..6....w..e...*..{..az8OAYewNgELvwQrvCQFNi4j455hRwuI26KpqTgc{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\NJ1L9FBN\www.google[1].xml	
Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	511
Entropy (8bit):	7.498387653476751
Encrypted:	false
SSDEEP:	12:Jc1hZK70/56MeSe2ooT+ySA6XAxQks7S+VFabcii9a:J+hg7GgMe9o+ySA6XAWVSIbbD
MD5:	29875D8F40B4F270282A9AC12F641A92
SHA1:	9BF9176FC8E4ABE6FA353268404F0F1F8320AA95
SHA-256:	57357818E56E5E2F9E33F67CB6DCCDF0BB9887B729C277B7DE6879C284E0CAD7
SHA-512:	8A14481DABCFF6ABF499EDA63C11FD87213D81A3F4BCD10B967FA8541143C979D3A0F6C6CF941518B4CE4FFB8C4A39D63B5FB6EE79C65D386AF017B9F756D8 24
Malicious:	false
Reputation:	unknown
Preview:	<root..h.R.jE....PX.....-h.....O.....(....^....B...A..T...!...i.r.}...y.....u..~..r=.." ...1.Q;..ZoA.Xr(.a.....L.....^.....2...CNC..f.%2.PS`..g.]...L^..6.....6`....=...o..j.0..v.O0.F.:G.H..T\f4 t...a.AQ-....8.R*r*...7...."t...g...B|..."1d.f....+.....y..}. .|Dd..1..#xx.*.j.q..8..j..x.....l..i.&..?f.../+.0..v.h...[i1..i.....E.....O.UAB..x2..&..?C.NuHw'..a3.u_.c.e..}L.V.<.Y~...l..@....$H.... ...].TZ..Raz8OAYewNgELvwQrvCQFNi4j455hRwuI26KpqTgc{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\NJ1L9FBN\www.google[1].xml.vapo (copy)	
Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	511
Entropy (8bit):	7.498387653476751

Encrypted:	false
SSDEEP:	12:Jc1hZK70/56MeSe2ooT+ySA6XAxQks7S+VFabcii9a:J+hg7GgMe9o+ySA6XAWVSIlbbD
MD5:	29875D8F40B4F270282A9AC12F641A92
SHA1:	9BF9176FC8E4ABE6FA353268404F0F1F8320AA95
SHA-256:	57357818E56E5E2F9E33F67CB6DCCDF0BB9887B729C277B7DE6879C284E0CAD7
SHA-512:	8A14481DABCFF6ABF499EDA63C11FD87213D81A3F4BCD10B967FA8541143C979D3A0F6C6CF941518B4CE4FFB8C4A39D63B5FB6EE79C65D386AF017B9F756D8 24
Malicious:	false
Reputation:	unknown
Preview:	<root..h.R.jE....PX.....-h.....O.....(....^....B...A..T...!...i.r.}...y.....u..~..r=.." ...1.Q;..ZoA.Xr(.a.....L.....^.....2...CNC..f.%2.PS`..g.]...L^..6.....6`....=...o..j.0..v.O0.F.:G.H..T\f4 t...a.AQ-....8.R*r*...7...."t...g...B|..."1d.f....+.....y..}. .|Dd..1..#xx.*.j.q..8..j..x.....I..i.&..?f.../+.0..v.h...[i1..i.....E.....O.UAB..x2..&..?C.NuHw'..a3.u_.c.e..}L.V.<.Y~...I..@....$H.... ...].TZ..Raz8OAYewNgELvwQrvCQFNi4j455hRwuI26KpqTgc{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\WP4N5YVD\contextual.media[1].xml

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	500
Entropy (8bit):	7.559696518079612
Encrypted:	false
SSDEEP:	12:Txhl0d2aTdwRNNKyZALykpMYKM3wOel28VXUrbWcii9a:tk4nZSbMY73wOESabD
MD5:	1C748AAA107E799BD4F898648C953575
SHA1:	6CDE9B528E5CF7F7710D506EA40B3849DD2D9206
SHA-256:	16852F3D3B21C912D852A3C6974465F4CCC234D2A6D2ED1087C194408F79347B
SHA-512:	63CB1331EBC9724A23E3080344117B94D7BAE4CB7F6032A6ADC85EF18461D2164323A542C34B661AB584A3980F4D3349215718 85BF7ED27DED885E888A7C5F58
Malicious:	false
Reputation:	unknown
Preview:	<rootT....XD{..._....4....;.../.}#..?.....>....5n.;?....q...Z)...*....OO..F.a.l...\....32Zmh..y.l..6..w....(.N.fl..^.(.....n..<..*~.E..\.....h..wg...W.....H..D..x..H@..!.(..P.ez...F.R.."r.vrY.Q..q... D..d..,E..6.<!.....,X.9.X`,F7%E.....*.3YA.i,j....F... &.=.....~.Q.i:....Vg....w.\.t.....GW..K.j.s..2.....C..Y...I...'19...e.MR..g.K.F./r...=.....\.A+Xf.dB.X..9D.~!.-.OQ....:.H.Wdv.%...o .be....-]az8OAYewNgELvwQrvCQFNi4j455hRwuI26KpqTgc{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\WP4N5YVD\contextual.media[1].xml.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	500
Entropy (8bit):	7.559696518079612
Encrypted:	false
SSDEEP:	12:Txhl0d2aTdwRNNKyZALykpMYKM3wOel28VXUrbWcii9a:tk4nZSbMY73wOESabD
MD5:	1C748AAA107E799BD4F898648C953575
SHA1:	6CDE9B528E5CF7F7710D506EA40B3849DD2D9206
SHA-256:	16852F3D3B21C912D852A3C6974465F4CCC234D2A6D2ED1087C194408F79347B
SHA-512:	63CB1331EBC9724A23E3080344117B94D7BAE4CB7F6032A6ADC85EF18461D2164323A542C34B661AB584A3980F4D3349215718 85BF7ED27DED885E888A7C5F58
Malicious:	false
Reputation:	unknown
Preview:	<rootT....XD{..._....4....;.../.}#..?.....>....5n.;?....q...Z)...*....OO..F.a.l...\....32Zmh..y.l..6..w....(.N.fl..^.(.....n..<..*~.E..\.....h..wg...W.....H..D..x..H@..!.(..P.ez...F.R.."r.vrY.Q..q... D..d..,E..6.<!.....,X.9.X`,F7%E.....*.3YA.i,j....F... &.=.....~.Q.i:....Vg....w.\.t.....GW..K.j.s..2.....C..Y...I...'19...e.MR..g.K.F./r...=.....\.A+Xf.dB.X..9D.~!.-.OQ....:.H.Wdv.%...o .be....-]az8OAYewNgELvwQrvCQFNi4j455hRwuI26KpqTgc{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\YU3ONM33\www.microsoft[1].xml

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	7.566688643940721
Encrypted:	false
SSDEEP:	12:RV9t8EXN2KtjYJHVsAeKDD2QHuHdbchc10WfDMKPPw/ucii9a:rP8m/tjYJHVzD2BHLbIWbD
MD5:	3C4CA7203850061CC6ED41DF3BCFE07D
SHA1:	BA1160F4BD457E7469307DE35026CC655C36BCBC
SHA-256:	770F083EDBD9A70E5FE3DF6DF2C913E9381AFA605394452AAC37953AF6B22541

SHA-512:	4BBD5626498EF2EAF97461CC3842F8C323E2DEEFCEF4BA24EF77F551AEDC13206A9D26EE340BA72C0DEBD65199A507B9D94AE5E8A8C299CB3003E724E1D78EED
Malicious:	false
Reputation:	unknown
Preview:	<root&.c...S.r..{..._.b.E.W>..a.>..F.....V$4.....N{.O...B&..1.s*4...fl.,..A.hdWel..0....)}....Dh.a...c..`.M.....w..o.t)k.4..[.z.k6..~.....@O.....Yy.G....T=.4.....1..K....m.e .y.H.....:...01ag.V.F.0..R.....}.*..5..z.#.8_vy....*.T.....}....."t.4@O>.X.. .dR./(.M.m.=wY.?.!.-...v.'.(.No.q..^.K..,.$..y...P.w...BDAx58...y.@.....aq8-.j.}S]..#..b....`hc..;..$R..f.r xL...k...*j-9.9~Rg.6..I...o...b....._..p.O@..H.r..-^....L....Rp.Uq.B..O|.,Y"5ew...9.az8OAYewNgELvwQrvCQFNi4j455hRwuI26KpqTgc{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\YU3ONM33\www.microsoft[1].xml.vapo (copy)	
Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	7.566688643940721
Encrypted:	false
SSDEEP:	12:RV9t8EXN2KtjYJHVsAeKDD2QHuHdbchc10WfDMKPPw/ucii9a:rP8m/tjYJHVzD2BHLbIWbD
MD5:	3C4CA7203850061CC6ED41DF3BCFE07D
SHA1:	BA1160F4BD457E7469307DE35026CC655C36BCBC
SHA-256:	770F083EDBD9A70E5FE3DF6DF2C913E9381AFA605394452AAC37953AF6B22541
SHA-512:	4BBD5626498EF2EAF97461CC3842F8C323E2DEEFCEF4BA24EF77F551AEDC13206A9D26EE340BA72C0DEBD65199A507B9D94AE5E8A8C299CB3003E724E1D78EED
Malicious:	false
Reputation:	unknown
Preview:	<root&.c...S.r..{..._.b.E.W>..a.>..F.....V$4.....N{.O...B&..1.s*4...fl.,..A.hdWel..0....)}....Dh.a...c..`.M.....w..o.t)k.4..[.z.k6..~.....@O.....Yy.G....T=.4.....1..K....m.e .y.H.....:...01ag.V.F.0..R.....}.*..5..z.#.8_vy....*.T.....}....."t.4@O>.X.. .dR./(.M.m.=wY.?.!.-...v.'.(.No.q..^.K..,.$..y...P.w...BDAx58...y.@.....aq8-.j.}S]..#..b....`hc..;..$R..f.r xL...k...*j-9.9~Rg.6..I...o...b....._..p.O@..H.r..-^....L....Rp.Uq.B..O|.,Y"5ew...9.az8OAYewNgELvwQrvCQFNi4j455hRwuI26KpqTgc{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe	
Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	335360
Entropy (8bit):	7.226981815045936
Encrypted:	false
SSDEEP:	6144:KYZSitAsJ2xdN5B3TurOnuQdTLOOEPHg:KToAsJ2XNXuStOOuH
MD5:	B888EFE68F257AA2335ED9CBD63C1343
SHA1:	C1A97D41D16A7A274802E873CE6B990312B07E03
SHA-256:	C8B5119160D3301FC69657F1C23C8561E6290B953EC645298F436431D41BBD70
SHA-512:	7D5BFC95C8F3D5BCC12A4AE1929B4FF946AB3747B29B3AB57B684DECFA78DB4836EC187D8A9ECDA5D2E6C4BAA02989AC1648FB9AAA0E592FB3A70F880529E3A8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 87%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.S.....B?.....z9.....z.....z.....t4.....z.....z=.....z :.....Rich.....PE..L.....c.....T....+.....w.....p....@.....Y..P.....,(-.....XC ..@.....text....S.....T..... ..`.data...lH+..p.....X.....@....rsrc...(-....,.....@..@..... ....

C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build3.exe	
Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9728
Entropy (8bit):	5.3362059272001
Encrypted:	false
SSDEEP:	192:9UEc8b6H1LE+4LoGgMatAJ2lzUw317NyEpvNHhqyo:9UUE1BYoGza/D3170kiyo
MD5:	9EAD10C08E72AE41921191F8DB39BC16
SHA1:	ABE3BCE01CD34AFC88E2C838173F8C2BD0090AE1
SHA-256:	8D7F0E6B6877BDFB9F4531AFAFD0451F7D17F0AC24E2F2427E9B4ECC5452B9F0

SHA-512:	AA35DBC59A3589DF2763E76A495CE5A9E62196628B4C1D098ADD38BD7F27C49EDF93A66FB8507FB746E37EE32932DA2460E440F241ABE1A5A279ABCC1E5FFE4A
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Clipboard_Hijacker, Description: Yara detected Clipboard Hijacker, Source: C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build3.exe, Author: Joe Security • Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build3.exe, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build3.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 88%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o.....o.....Rich.....PE..L.....a..... .....0....@.....`.....@.....:..<.....P.,....9..8.....0..0.....text..... ..... ..`.rdata.....0.....@..@.data...`....@.....@....reloc..,....P.....".....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\3C54.exe.log

Process:	C:\Users\user\AppData\Local\Temp\3C54.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD3D
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\build2[1].exe

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	335360
Entropy (8bit):	7.226981815045936
Encrypted:	false
SSDEEP:	6144:KYZSitAsJ2xdN5B3TurOnuQdTLOOEPHg:KToAsJ2XNXuStOOuH
MD5:	B888EFE68F257AA2335ED9CBD63C1343
SHA1:	C1A97D41D16A7A274802E873CE6B990312B07E03
SHA-256:	C8B5119160D3301FC69657F1C23C8561E6290B953EC645298F436431D41BBD70
SHA-512:	7D5BFC95C8F3D5BCC12A4AE1929B4FF946AB3747B29B3AB57B684DECFA78DB4836EC187D8A9ECDA5D2E6C4BAA02989AC1648FB9AAA0E592FB3A70F880529E3A8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 87%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.S.....B?.....z9.....z.....z.....t4.....z.....z=.....z :.....Rich.....PE..L.....c.....T....+.....w.....p....@.....Y..P.....,(-.....XC ..@.....text....S.....T..... ..`.data...lH+..p.....X.....@....rsrc...(-....,.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\build3[1].exe

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9728

Entropy (8bit):	5.3362059272001
Encrypted:	false
SSDEEP:	192:9UEc8b6H1LE+4LoGgMatAJ2lzUw317NyEpvNHhqyo:9UUE1BYoGza/D3170kiyo
MD5:	9EAD10C08E72AE41921191F8DB39BC16
SHA1:	ABE3BCE01CD34AFC88E2C838173F8C2BD0090AE1
SHA-256:	8D7F0E6B6877BDFB9F4531AFAFD0451F7D17F0AC24E2F2427E9B4ECC5452B9F0
SHA-512:	AA35DBC59A3589DF2763E76A495CE5A9E62196628B4C1D098ADD38BD7F27C49EDF93A66FB8507FB746E37EE32932DA2460E440F241ABE1A5A279ABCC1E5FFE4A
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Clipboard_Hijacker, Description: Yara detected Clipboard Hijacker, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\build3[1].exe, Author: Joe Security • Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\build3[1].exe, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\build3[1].exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 88%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o.....o.....Rich.....PE..L.....a..... .....0....@.....`.....@.....:..<.....P.,....9..8.....0..0.....text..... ..... ..`.rdata.....0.....@..@.data...`....@.....@....reloc..,....P.....".....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll

Process:	C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1074176
Entropy (8bit):	6.478034514486552
Encrypted:	false
SSDEEP:	24576:YVaH8jJPWhQnZzrZ+7xr1rZfVlTxd43v7t5m:2AhQnZzrZSxxZfVlUD
MD5:	16FD83A682162D6EDC119DC12C9990DC
SHA1:	4B5F38C78C8E5F1333989DA0912E945335F82C95
SHA-256:	36BE2F6CCCDF3EDC709E7DABCBE529D4F6390D3C624BA10FB471BD05D36060C8
SHA-512:	5AF414C95DB738D0A65FDD67F2FF3923C451EE68856237F55626586AAC14EFE62288F5B8D74A5FBF2EABA9E6A1689CEA89B856212A597AB12A3A4B0097E3F3A5
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll, Author: Joe Security • Rule: OlympicDestroyer_1, Description: OlympicDestroyer Payload, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll, Author: kevoreilly
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 83%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sO..sO..sO..wN..sO..pN..sO..vNe.sO..vN..sO..wN..sO..pN.. sO..rN..sO..rOi.sON.zN..sON.sN..sON..O..sON.qN..sORich..sO.....PE..d....T.c....." .....H.....`..... `{..X....{.....h.....p.....text..... ..`.rdata.....@..@.data....o.....6...|..... ....@....pdata.....@..@_RDATA.....J.....@..@.rsrc.....L.....@..@.reloc..h.....N.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\get[1].htm

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	560
Entropy (8bit):	6.009613601911672
Encrypted:	false
SSDEEP:	12:YGJ68UiiMLwLR8AFq5I5WhsRtCV64uzR5W:YgJUFfFxg0cV/MI
MD5:	9252E3DCF847925C8080204C028EBAE6
SHA1:	498661D45D44EDED195FBB98AEC310D87BF1947E
SHA-256:	2ED806DEEF0185D3983A46422B07B33CB62FF04873066C7E315876C644B4D4D8
SHA-512:	71970EFCE4E86B1415696A792DC595F7E9993A587B34D4E000677B8C647A6CDE43845B7E1EBE3EE7F54D0937D2D42B4F8C3ED1C7F4468D2BF8392D57E3A6253
Malicious:	false

Reputation:	unknown
Preview:	{"public_key":"-----BEGIN PUBLIC KEY-----\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzVVm4tu5iyZw13a\/GiU0\\nV5T6yum3k8oXJuPfu\/dlDp5n6Tzk6N8vnuKpjC8lkV7xuMYgdtfQ4cWYKxUvBMa5\\nZoYlzVSlrIVedQM2wz2yOUQcOloagsxQEzv9Of3rNy2gF4dr82Kp8laqDk0c3hjz\\nmazDrTR\/jjRhNxY80qI9FZk8pFyou7p\/wowlaHHEiFkCdD2yrZBW1b8jmpuEPqdm\\nH+Nas4N51zRvyqkWCKO68bPnX70ZcR1zLiCfJNxJJ\/wx\/uRwZXCJW3Mhdz+bwMqd\\nhECMff6Chw2XhPIKlGEHGhqCwRLO+yfVnjAF8Tu6hWIg7qhC0tx1sT2u6Xy02NLT\\ntQIDAQAB\\n-----END PUBLIC KEY-----\\n","id":"az8OAYewNgELvwQrvCQFNi4j455hRwuI26KpqTgc"}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\image[1].jpg

Process:	C:\Users\user\AppData\Local\Temp\aafg31.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1080x1440, components 3
Category:	dropped
Size (bytes):	1495756
Entropy (8bit):	6.930675293414024
Encrypted:	false
SSDEEP:	24576:SMaEt+i3Co+P2EtMd28BWh70vLLvtfSQxMXBcdpOH+BEgkuTun:SIoi/Ete28BNsQxMOpPr8
MD5:	6DB41995F1C0E3EC9C8F98409B9F159E
SHA1:	0F6D188A74EB7D36566F76E1A7CE3ADB68C4EB39
SHA-256:	0329E9CC62E46495BAFCCF5550E10BAD608A7A262160AD4730D8E049377457E0
SHA-512:	F38AD19CD98B6A8B8158FFDCEF54D53A60F2DE4CE29676DE3592BF9BB6F34E12111504ADD92892E9939439DBB464D54422ABB1905C9961C0628643316DEDAF A
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....C.....C.....8.....c.....!.."1A.2Q.#BR aq3br.....$4CS...c....%s.....&5DTd..'6EUet....7F.....>.....!.1.A..."2Qa.#3q..B....$4...C.DRr.b.....?....{.e..#y.|.,....P.b...?...'(..+....#..... B....:,9=.o5...,b...M:,rP.w....<.C1.....&.....IP....OrP.rZ....P,M.y"...,.....@X..oD..@;: ,.....$...P.p.....pg....:.<.....;...8..B.....)..,.....a.. ..!.!0..r.P..*.....f.....O..t*...o.'...[.....o`h..4.m| ,..G....<<0@.?.F.*R7Sd...e.@.._.@...j..FGy.,..{..0.X..6.h7...E..wF..r..nl.Yp....o....j`..T...Y].7.m.J.a....g..@..,..<L.TD.Ra...u.....BS.\.....+><{N8.rA....G..#....n.....F.....|#.;....Bs..n 6....a..|..5d...g..|.w.4...}...I|....S..>.....aRW;~g..y.I4_)....)...(v.w.....]2.k}>P...^...|..=.c.u...V

C:\Users\user\AppData\Local\Temp\388B.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	288768
Entropy (8bit):	6.584915706285476
Encrypted:	false
SSDEEP:	3072:tiaWGvA5BMvdYuAJ2qiGD0swth9Ewaf/s7htn5gYTtic7:t4GvAMdj40th7a3s7SYTtic
MD5:	7A8E3D000FBA0F5765B98E2D78EB9D12
SHA1:	2DFF944F970FAEF5C6FA92AC8FBE82C9251553F3
SHA-256:	13744BE5698FFDDC96D55415FDEEBDE4921ED199B4174251D83F1FD5B5A05C66
SHA-512:	1D56B0DD129D7A1C1E76B110F9CEE4C63D2F021BCDCACA53CD780CC5E6B6CAFD6CEBC70FB62198910CAE2E4E9EA083216611923C72A4120FCC30CA3894A0 8DA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...|.....|.....|...H...EX..k...b.....|...c...|...c...|...c...Rich b.....PE..L...G..c.....~...'&.....YN.....@.....(.....d.....&.....(..... .....P1..@..... .....text....}.....~..... ..`.data...DX$.....@....rsrc.....&.....@..@.reloc...3....(..4...4.....@..B..... ....

C:\Users\user\AppData\Local\Temp\3C54.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	5129728
Entropy (8bit):	7.738068755959416
Encrypted:	false
SSDEEP:	98304:V127F4DH/LHW+MQ7TZeDTRFh0ZKzXqw8jY:quqkfadIZGXqvjY
MD5:	2AF03D52F9CF9E53DFFC1183B403E1B7
SHA1:	124D97058DB289DA50A48F90911BE2D67649F629
SHA-256:	A41F46EF947C9FF3B1E5625E6CF5799E776A55E48F54F7FFFE19E08E826DE99A
SHA-512:	7D773C689DC4DD3BE9807C00207CF2713767C77C2B25B9EEB47FA7C0F87E05FA3736D25D79B428771D0FDE6C0F25FCCC476589817AA7FA93E622230E75AD65 8

Malicious:	**true**
Yara Hits:	• Rule: MALWARE_Win_DLInjector04, Description: Detects downloader / injector, Source: C:\Users\user\AppData\Local\Temp\3C54.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 70%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....pd.....<N.....ZN.. ...`N...@.. ..... N.....@.....PZN.K....`N.....N..... ....H.....text....:N.. ...<N..... ..`.rsrc.....`N.....>N..... ..@..@.reloc.....N.....DN.....@..B.....ZN.....H.....DN.\.....'....N.....0..._.....~....,(.....(....~.....(.....(....~.....(.....(....~.....(.....(

C:\Users\user\AppData\Local\Temp\3E02.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	599040
Entropy (8bit):	7.518690203928315
Encrypted:	false
SSDEEP:	12288:sdhllTZXaG2MjEkQyX7ev9DgST8jIgxATGG56aETtiE:whlf52MjEtyaDrvyAT352EE
MD5:	917FFF16528EF56F427E0B87261D9DD3
SHA1:	BC80314877D5E307CB62F87DAB900DEBE4DDD252
SHA-256:	0119E5129B4785669608345082D862F01474994A566AA8D225A730F4BF38D4D5
SHA-512:	9B1775B994A952D940582E6CDB7775C06226C196DC0DAABFD35DD61634FDAAA8CD43715D593FF8CB7C23C2B10E140E7E5D5A13BA04588B062FD53AF6B88216FE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...|.....|.....|...H...EX..k...b.....|...c...|...c...|...c...Rich b.....PE..L.....a.....6...&&.....YN.....P....@.....-.....:..d.....+.....P-..... .....P1..@..... .....text....5.....6..... ..`.data...DX$..P.....:.....@....rsrc.....+.....X.....@..@.reloc..&6...P-..8.....@..B..... ....

C:\Users\user\AppData\Local\Temp\57DC.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	503808
Entropy (8bit):	7.379104304802616
Encrypted:	false
SSDEEP:	6144:e1z0CQa13pdiPumUtZVUqkj+VOVGakSEPhVHUk9ZuyxPwF7XgivTtiuy:eV0CQa131t1keBSEPHHUSu5tTtiuy
MD5:	57DD320EAE0FADD155619407C8B5313C
SHA1:	FC2CE4B86D64025DBBA19BB84E561A27FCB6FFB3
SHA-256:	4A524E63C81E6CF9AB8A86F8DE0973EA6A6D0973545867D34EBA1B777E238628
SHA-512:	23F1E1833A6A52D28CCE3B07C726D568C2743B76593E46BA18CD97C7F3F29C262EA3624D7A3F0E745A6F776E0C21421E2A5A7541783FBCF1D31B359843436DD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 43%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...|.....|.....|...H...EX..k...b.....|...c...|...c...|...c...Rich b.....PE..L.....pb.....$&.....YN.....@..... ,.....W.....d....@*.....+..... .....P1..@..... .....text...z..... ..`.data...DX$.....@....rsrc.....@*.....@..@.reloc..@5....+..6...z.....@..B..... ....

C:\Users\user\AppData\Local\Temp\5DA0.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	5129728
Entropy (8bit):	7.738068755959416
Encrypted:	false
SSDEEP:	98304:V127F4DH/LHW+MQ7TZeDTRFh0ZKzXqw8jY:quqkfadIZGXqvjY

MD5:	2AF03D52F9CF9E53DFFC1183B403E1B7
SHA1:	124D97058DB289DA50A48F90911BE2D67649F629
SHA-256:	A41F46EF947C9FF3B1E5625E6CF5799E776A55E48F54F7FFFE19E08E826DE99A
SHA-512:	7D773C689DC4DD3BE9807C00207CF2713767C77C2B25B9EEB47FA7C0F87E05FA3736D25D79B428771D0FDE6C0F25FCCC476589817AA7FA93E622230E75AD658
Malicious:	**true**
Yara Hits:	• Rule: MALWARE_Win_DLInjector04, Description: Detects downloader / injector, Source: C:\Users\user\AppData\Local\Temp\5DA0.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 70%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....pd.....<N.....ZN.. ...`N...@.. ..... N.....@.....PZN.K....`N.....N..... ....H.....text....:N.. ...<N..... ..`.rsrc.....`N.....>N..... ..@..@.reloc.....N.....DN.....@..B.....ZN.....H.....DN.\.....'....N.....0..._.....~.....(.....(....~.....(.....(....~.....(.....(....~.....(.....(....~.....(....~.....~.... ....Z(....~.....r...pr...p.(....&..8....~.....o.....~.....o.....~.....o.....~.....o.....(.....~.....(.....~....r...p(.....(....r...po.....(.....+)~....r1..p(.....(....r...po....(.....(....(..... (.....(.....X..~....o....?....~....&*..0../.....s.....s.....s.....o.....,,

C:\Users\user\AppData\Local\Temp\673.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	288768
Entropy (8bit):	6.584915706285476
Encrypted:	false
SSDEEP:	3072:tiaWGvA5BMvdYuAJ2qiGD0swth9Ewaf/s7htn5gYTtic7:t4GvAMdj40th7a3s7SYTtic
MD5:	7A8E3D000FBA0F5765B98E2D78EB9D12
SHA1:	2DFF944F970FAEF5C6FA92AC8FBE82C9251553F3
SHA-256:	13744BE5698FFDDC96D55415FDEEBDE4921ED199B4174251D83F1FD5B5A05C66
SHA-512:	1D56B0DD129D7A1C1E76B110F9CEE4C63D2F021BCDCACA53CD780CC5E6B6CAFD6CEBC70FB62198910CAE2E4E9EA083216611923C72A4120FCC30CA3894A08DA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b.....PE..L...G..c.....~..."&.....YN.....@.....(.....d.....&.....(..... .....P1..@..... .....text....}.....~..... ..`.data...DX$.....@....rsrc.....&.....@..@.reloc...3....(..4...4.....@..B..... ....

C:\Users\user\AppData\Local\Temp\6FA9.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	5129728
Entropy (8bit):	7.738068755959416
Encrypted:	false
SSDEEP:	98304:V127F4DH/LHW+MQ7TZeDTRFh0ZKzXqw8jY:quqkfadIZGXqvjY
MD5:	2AF03D52F9CF9E53DFFC1183B403E1B7
SHA1:	124D97058DB289DA50A48F90911BE2D67649F629
SHA-256:	A41F46EF947C9FF3B1E5625E6CF5799E776A55E48F54F7FFFE19E08E826DE99A
SHA-512:	7D773C689DC4DD3BE9807C00207CF2713767C77C2B25B9EEB47FA7C0F87E05FA3736D25D79B428771D0FDE6C0F25FCCC476589817AA7FA93E622230E75AD658
Malicious:	**true**
Yara Hits:	• Rule: MALWARE_Win_DLInjector04, Description: Detects downloader / injector, Source: C:\Users\user\AppData\Local\Temp\6FA9.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 70%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....pd.....<N.....ZN.. ...`N...@.. ..... N.....@.....PZN.K....`N.....N..... ....H.....text....:N.. ...<N..... ..`.rsrc.....`N.....>N..... ..@..@.reloc.....N.....DN.....@..B.....ZN.....H.....DN.\.....'....N.....0..._.....~.....(.....(....~.....(.....(....~.....(.....(....~.....(....~.....~.... ....Z(....~.....r...pr...p.(....&..8....~.....o.....~.....o.....~.....o.....~.....o.....(.....~.....(.....~....r...p(.....(....r...po.....(.....+)~....r1..p(.....(....r...po....(.....(....(..... (.....(.....X..~....o....?....~....&*..0../.....s.....s.....s.....o.....,,

C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe

Process:	C:\Users\user\AppData\Local\Temp\NewPlayer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	255488
Entropy (8bit):	6.3672540076726225
Encrypted:	false
SSDEEP:	6144:W9ynaiEzdOYqdjqqMth9iiry6Q2lbiiRWu1i5bDuPmyye:yWcmAh9ix2r1u1ile
MD5:	08240E71429B32855B418A4ACF0E38EC
SHA1:	B180ACE2EA6815775D29785C985B576DC21B76B5
SHA-256:	A41B4591C7351562ED9125DA2C93DB246E87E05198D2EC0951733D1919E119D8
SHA-512:	69FA8CAE9BF69BCC498CFD7AF08FCDFD299440BA0DD679835CC8EA14F07B0346F965F88350A5261F2312E046B0DD498B8453D647B5F023762E4265FFA47472B
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 88%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z....D...D...D...E...D...EG..D...E...D2..E...D2..E...D2..E...D...E...D...DE..D|..E...D|..D...D|..E...DRich...D.....PE..L....T.c.....u.....@.....@.....@.....@.....0.....*..0p..p.....Dq.....p..@.....d.....text..... ..`.rdata.....@..@.data....D.....@....rsrc.....@..@.rel oc...*.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\853321935212

Process:	C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, components 3
Category:	dropped
Size (bytes):	96926
Entropy (8bit):	7.918189757438893
Encrypted:	false
SSDEEP:	1536:Cf0zfAYPjM2DR2hqkyycWq4lvY2QcdOrVUxwAQFBG7jZy3X40wzKqRB0QzYubCKa:X7bjM2D08huQcdS0sBGo3Z45znbCK6qe
MD5:	7D553C2E447C480D12E974789BD25005
SHA1:	3F3FA3E0E8EC8824DE8C0B9958EDF9D5E2D431BB
SHA-256:	343F4273AF9F9D7E845AFAE56851D1964F508D239A87796B2BA05BE9B7D695DF
SHA-512:	BB0268A0F155C0B7D1D7EBE36567B8882BC188D3B94A5640D4224BE8A9309EE5E5CABB63D23EDF76F320D2D825DA4326572FD033F18B8750613468FC33E9104A
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\...x....Mj}9oE...7....*.....]..(...x..:.e...+..6..r.....#XP.Q^(.*uz.....G...V_.~....3.c.o.?g.....z.8...Q...9(.Z.'.C...U...5..+....)h...i)M.,c.%}=g._.w.6..i"W!n_. .Z..... .....7.R>\..W.W.....gu.8..7-...._....'...^X....+u1.....n..J.QKIZ.-%.P.b.Z....>.....4+..b.Y&..F...)Pq.L..... .....H.#.|..).?.H.'.|....).?m.....h.t.....|4.%...

C:\Users\user\AppData\Local\Temp\913F.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	809984
Entropy (8bit):	7.646586492015294
Encrypted:	false
SSDEEP:	12288:6aBz+gzWrFGCkY9J22msYEy85LJxg1YSlniLs4CEhtYdGJ+CejE:/z+gzW7Z22byv1YSsA4CpdGJ+I
MD5:	15BC205C2CAF7196EE2267087C3B2BB8
SHA1:	0E1EE7E4CCAFD5A62D6B2B3A9369709EAB0E1F0B
SHA-256:	FDEE1B99A95C5DFB4A256CDB7E43CE3F21A5D2C2977CE252AAFFA77A9E017DDF
SHA-512:	DBFD1C50D16F21084B542A2ABD2B35F6489D30B55E9B5B8DC9014BCC9C4AE8A24DF08A659B28EAD862291BC65107A34C0CDA8CAD08A354E92FA23138D21F62C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 71%
Reputation:	unknown

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b..........PE..L.....b.....L...H&.....9N.....`....@.....0.....4.....XO..d.....0.....0..... .....1..@..... .....text....J.....L..... ..`.data...DX$..`.....P.....@....rsrc...0.....n.....@..@.reloc.."8....0..:.."..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\9F31.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	5129728
Entropy (8bit):	7.738068755959416
Encrypted:	false
SSDEEP:	98304:V127F4DH/LHW+MQ7TZeDTRFh0ZKzXqw8jY:quqkfadIZGXqvjY
MD5:	2AF03D52F9CF9E53DFFC1183B403E1B7
SHA1:	124D97058DB289DA50A48F90911BE2D67649F629
SHA-256:	A41F46EF947C9FF3B1E5625E6CF5799E776A55E48F54F7FFFE19E08E826DE99A
SHA-512:	7D773C689DC4DD3BE9807C00207CF2713767C77C2B25B9EEB47FA7C0F87E05FA3736D25D79B428771D0FDE6C0F25FCCC476589817AA7FA93E622230E75AD658
Malicious:	**true**
Yara Hits:	• Rule: MALWARE_Win_DLInjector04, Description: Detects downloader / injector, Source: C:\Users\user\AppData\Local\Temp\9F31.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 70%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....pd.....<N.....ZN.. ...`N...@.. ..... N.....@.....PZN.K....`N.....N..... ....H.....text....:N.. ...<N..... ..`.rsrc.....`N.....>N..... ..@..@.reloc.....N.....DN.....@..B.....ZN.....H.....DN.\.....'....N.....0._.....~.....(.....(....~.....(.....(....~.....(.....(....~.....(.....(....~....,~.... ....Z(....~....,r...pr...p.(....&..8...~.....o.....~.....o.....~.....o.....~.....o.....(.....~....,...(.....~....r...p(.....,(....r...po.....(.....+)~....r1..p(.....,(....r…po....(.....(....(..... (.....(.....X..~....o....?....~....&*..0../.....s.....s.....s.....o......,

C:\Users\user\AppData\Local\Temp\A170.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	809984
Entropy (8bit):	7.646586492015294
Encrypted:	false
SSDEEP:	12288:6aBz+gzWrFGCkY9J22msYEy85LJxg1YSlniLs4CEhtYdGJ+CejE:/z+gzW7Z22byv1YSsA4CpdGJ+I
MD5:	15BC205C2CAF7196EE2267087C3B2BB8
SHA1:	0E1EE7E4CCAFD5A62D6B2B3A9369709EAB0E1F0B
SHA-256:	FDEE1B99A95C5DFB4A256CDB7E43CE3F21A5D2C2977CE252AAFFA77A9E017DDF
SHA-512:	DBFD1C50D16F21084B542A2ABD2B35F6489D30B55E9B5B8DC9014BCC9C4AE8A24DF08A659B28EAD862291BC65107A34C0CDA8CAD08A354E92FA23138D21F62C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 71%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b..........PE..L.....b.....L...H&.....9N.....`....@.....0.....4.....XO..d.....0.....0..... .....1..@..... .....text....J.....L..... ..`.data...DX$..`.....P.....@....rsrc...0.....n.....@..@.reloc.."8....0..:.."..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\A3D5.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	809984
Entropy (8bit):	7.646586492015294
Encrypted:	false
SSDEEP:	12288:6aBz+gzWrFGCkY9J22msYEy85LJxg1YSlniLs4CEhtYdGJ+CejE:/z+gzW7Z22byv1YSsA4CpdGJ+I
MD5:	15BC205C2CAF7196EE2267087C3B2BB8
SHA1:	0E1EE7E4CCAFD5A62D6B2B3A9369709EAB0E1F0B

SHA-256:	FDEE1B99A95C5DFB4A256CDB7E43CE3F21A5D2C2977CE252AAFFA77A9E017DDF
SHA-512:	DBFD1C50D16F21084B542A2ABD2B35F6489D30B55E9B5B8DC9014BCC9C4AE8A24DF08A659B28EAD862291BC65107A34C0CDA8CAD08A354E92FA23138D21F62C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 71%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b.....PE..L.....b.....L...H&.....9N.....`....@.....0.....4.....XO..d.....0.....0..... .....1..@..... .....text....J.....L..... ..`.data...DX$..`.....P.....@....rsrc...0.....n.....@..@.reloc.."8....0..:..."..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\B46F.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	802304
Entropy (8bit):	7.685061735084475
Encrypted:	false
SSDEEP:	24576:6nRTyltqh7DLUjjuiX+tR+WoXeAWG1qzz5E:8TZta/Uja7siAW
MD5:	6944FCA258A9009F9D3B7212CDB4874D
SHA1:	1E20555089B3D2B9E34B44422C8E6C3061E68F0E
SHA-256:	D34D06CCD3BA7877664E4769FF708D7C412EE5F43A76F2A2CE962C843CC5C35B
SHA-512:	A05299352297160D62FB91A75EC7D30E8C00CDAB97BFEF112429B0CED6041A3E6FB232686FF6A4080E9C98797B4D224792C6339600084DED4B12B0595575EDC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b.....PE..L....4.a.....N...(&.....YN.....`....@.....0.....Q..d.....`0..... .....P1..@..... .....text...JL.....N..... ..`.data...DX$..`.....R.....@....rsrc.....p.....@..@.reloc...8...`0..:.....@..B..... ....

C:\Users\user\AppData\Local\Temp\B8C8.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	809984
Entropy (8bit):	7.646586492015294
Encrypted:	false
SSDEEP:	12288:6aBz+gzWrFGCkY9J22msYEy85LJxg1YSlniLs4CEhtYdGJ+CejE:/z+gzW7Z22byv1YSsA4CpdGJ+I
MD5:	15BC205C2CAF7196EE2267087C3B2BB8
SHA1:	0E1EE7E4CCAFD5A62D6B2B3A9369709EAB0E1F0B
SHA-256:	FDEE1B99A95C5DFB4A256CDB7E43CE3F21A5D2C2977CE252AAFFA77A9E017DDF
SHA-512:	DBFD1C50D16F21084B542A2ABD2B35F6489D30B55E9B5B8DC9014BCC9C4AE8A24DF08A659B28EAD862291BC65107A34C0CDA8CAD08A354E92FA23138D21F62C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 71%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b.....PE..L.....b.....L...H&.....9N.....`....@.....0.....4.....XO..d.....0.....0..... .....1..@..... .....text....J.....L..... ..`.data...DX$..`.....P.....@....rsrc...0.....n.....@..@.reloc.."8....0..:..."..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\BC2.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	802304
Entropy (8bit):	7.685061735084475
Encrypted:	false

SSDEEP:	24576:6nRTyltqh7DLUjjuiX+tR+WoXeAWG1qzz5E:8TZta/Uja7siAW
MD5:	6944FCA258A9009F9D3B7212CDB4874D
SHA1:	1E20555089B3D2B9E34B44422C8E6C3061E68F0E
SHA-256:	D34D06CCD3BA7877664E4769FF708D7C412EE5F43A76F2A2CE962C843CC5C35B
SHA-512:	A05299352297160D62FB91A75EC7D30E8C00CDAB97BFEF112429B0CED6041A3E6FB232686FF6A4080E9C98797B4D224792C6339600084DED4B12B0595575EDC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b.....PE..L....4.a.....N...(&.....YN.....`....@.....0.....Q..d.....`0..... .....P1..@..... .....text...JL.....N..... ..`.data...DX$..`.....R.....@....rsrc.....p.....@..@.reloc...8...`0..:.....@..B..... ....

C:\Users\user\AppData\Local\Temp\C861.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	288768
Entropy (8bit):	6.584915706285476
Encrypted:	false
SSDEEP:	3072:tiaWGvA5BMvdYuAJ2qiGD0swth9Ewaf/s7htn5gYTtic7:t4GvAMdj40th7a3s7SYTtic
MD5:	7A8E3D000FBA0F5765B98E2D78EB9D12
SHA1:	2DFF944F970FAEF5C6FA92AC8FBE82C9251553F3
SHA-256:	13744BE5698FFDDC96D55415FDEEBDE4921ED199B4174251D83F1FD5B5A05C66
SHA-512:	1D56B0DD129D7A1C1E76B110F9CEE4C63D2F021BCDCACA53CD780CC5E6B6CAFD6CEBC70FB62198910CAE2E4E9EA083216611923C72A4120FCC30CA3894A0 8DA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b.....PE..L...G..c.....~...."&.....YN.....@.....(.....d.....&.....(..... .....P1..@..... .....text....}.....~..... ..`.data...DX$.....@....rsrc.....&.....@..@.reloc...3....(..4...4.....@..B..... ....

C:\Users\user\AppData\Local\Temp\CBE6.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	802304
Entropy (8bit):	7.685061735084475
Encrypted:	false
SSDEEP:	24576:6nRTyltqh7DLUjjuiX+tR+WoXeAWG1qzz5E:8TZta/Uja7siAW
MD5:	6944FCA258A9009F9D3B7212CDB4874D
SHA1:	1E20555089B3D2B9E34B44422C8E6C3061E68F0E
SHA-256:	D34D06CCD3BA7877664E4769FF708D7C412EE5F43A76F2A2CE962C843CC5C35B
SHA-512:	A05299352297160D62FB91A75EC7D30E8C00CDAB97BFEF112429B0CED6041A3E6FB232686FF6A4080E9C98797B4D224792C6339600084DED4B12B0595575EDC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b.....PE..L....4.a.....N...(&.....YN.....`....@.....0.....Q..d.....`0..... .....P1..@..... .....text...JL.....N..... ..`.data...DX$..`.....R.....@....rsrc.....p.....@..@.reloc...8...`0..:.....@..B..... ....

C:\Users\user\AppData\Local\Temp\D689.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	809984
Entropy (8bit):	7.646586492015294

Encrypted:	false
SSDEEP:	12288:6aBz+gzWrFGCkY9J22msYEy85LJxg1YSlniLs4CEhtYdGJ+CejE:/z+gzW7Z22byv1YSsA4CpdGJ+I
MD5:	15BC205C2CAF7196EE2267087C3B2BB8
SHA1:	0E1EE7E4CCAFD5A62D6B2B3A9369709EAB0E1F0B
SHA-256:	FDEE1B99A95C5DFB4A256CDB7E43CE3F21A5D2C2977CE252AAFFA77A9E017DDF
SHA-512:	DBFD1C50D16F21084B542A2ABD2B35F6489D30B55E9B5B8DC9014BCC9C4AE8A24DF08A659B28EAD862291BC65107A34C0CDA8CAD08A354E92FA23138D21F62C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 71%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b.....PE..L.....b.....L...H&.....9N.....`....@.....0.....4.....XO..d.....0.....0..... .....1..@..... .....text....J.....L..... ..`.data...DX$..`.....P.....@....rsrc...0.....n.....@..@.reloc.."8....0..:..."..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\D804.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	802304
Entropy (8bit):	7.685061735084475
Encrypted:	false
SSDEEP:	24576:6nRTyItqh7DLUjjuiX+tR+WoXeAWG1qzz5E:8TZta/Uja7siAW
MD5:	6944FCA258A9009F9D3B7212CDB4874D
SHA1:	1E20555089B3D2B9E34B44422C8E6C3061E68F0E
SHA-256:	D34D06CCD3BA7877664E4769FF708D7C412EE5F43A76F2A2CE962C843CC5C35B
SHA-512:	A05299352297160D62FB91A75EC7D30E8C00CDAB97BFEF112429B0CED6041A3E6FB232686FF6A4080E9C98797B4D224792C6339600084DED4B12B0595575EDC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b.....PE..L....4.a.....N...(&.....YN.....`....@.....0.....Q..d.....`0..... .....P1..@..... .....text...JL.....N..... ..`.data...DX$..`.....R.....@....rsrc.....p.....@..@.reloc...8...`0..:.....@..B..... ....

C:\Users\user\AppData\Local\Temp\EA44.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	802304
Entropy (8bit):	7.685061735084475
Encrypted:	false
SSDEEP:	24576:6nRTyItqh7DLUjjuiX+tR+WoXeAWG1qzz5E:8TZta/Uja7siAW
MD5:	6944FCA258A9009F9D3B7212CDB4874D
SHA1:	1E20555089B3D2B9E34B44422C8E6C3061E68F0E
SHA-256:	D34D06CCD3BA7877664E4769FF708D7C412EE5F43A76F2A2CE962C843CC5C35B
SHA-512:	A05299352297160D62FB91A75EC7D30E8C00CDAB97BFEF112429B0CED6041A3E6FB232686FF6A4080E9C98797B4D224792C6339600084DED4B12B0595575EDC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b.....PE..L....4.a.....N...(&.....YN.....`....@.....0.....Q..d.....`0..... .....P1..@..... .....text...JL.....N..... ..`.data...DX$..`.....R.....@....rsrc.....p.....@..@.reloc...8...`0..:.....@..B..... ....

C:\Users\user\AppData\Local\Temp\F4F7.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	288768
Entropy (8bit):	6.584915706285476
Encrypted:	false
SSDEEP:	3072:tiaWGvA5BMvdYuAJ2qiGD0swth9Ewaf/s7htn5gYTtic7:t4GvAMdj40th7a3s7SYTtic
MD5:	7A8E3D000FBA0F5765B98E2D78EB9D12
SHA1:	2DFF944F970FAEF5C6FA92AC8FBE82C9251553F3
SHA-256:	13744BE5698FFDDC96D55415FDEEBDE4921ED199B4174251D83F1FD5B5A05C66
SHA-512:	1D56B0DD129D7A1C1E76B110F9CEE4C63D2F021BCDCACA53CD780CC5E6B6CAFD6CEBC70FB62198910CAE2E4E9EA083216611923C72A4120FCC30CA3894A08DA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b.....PE..L...G..c.....~..."&.....YN.....@.....(.....d.....&.....(..... .....P1..@..... .....text....}.....~..... ..`.data...DX$.....@....rsrc.....&.....@..@.reloc...3....(..4...4.....@..B..... ....

C:\Users\user\AppData\Local\Temp\NewPlayer.exe

Process:	C:\Users\user\AppData\Local\Temp\3C54.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	255488
Entropy (8bit):	6.3672540076726225
Encrypted:	false
SSDEEP:	6144:W9ynaiEzdOYqdjqqMth9iiry6Q2lbiiRWu1i5bDuPmyye:yWcmAh9ix2r1u1ile
MD5:	08240E71429B32855B418A4ACF0E38EC
SHA1:	B180ACE2EA6815775D29785C985B576DC21B76B5
SHA-256:	A41B4591C7351562ED9125DA2C93DB246E87E05198D2EC0951733D1919E119D8
SHA-512:	69FA8CAE9BF69BCC498CFD7AF08FCDFD299440BA0DD679835CC8EA14F07B0346F965F88350A5261F2312E046B0DD498B8453D647B5F023762E4265FFA47472B
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Temp\NewPlayer.exe, Author: Joe Security
Antivirus:	• Antivirus: ReversingLabs, Detection: 88%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z....D...D...D...E...D...EG..D...E...D2..E...D2..E...D2..E...D...E...D ...DE..D|..E...D|..D...D|..E...DRich...D.....PE..L....T.c.....u.....@.....@.....@.....0.....*..0p..p..... .....Dq.....p..@.....d.....text..... ..`.rdata.....@..@.data....D.....@....rsrc.....@..@.rel oc...*.....,.....@..B..... .....

C:\Users\user\AppData\Local\Temp\XandETC.exe

Process:	C:\Users\user\AppData\Local\Temp\3C54.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	3890176
Entropy (8bit):	7.902408557753204
Encrypted:	false
SSDEEP:	49152:8Pu803iSM2N7aUjjqpEbUS2qv5MQBsSY/b7KoiTFUgxylC42lVJpiU71PP:s12BEE4vqxMQzub7OTFUgxylqTiU7J
MD5:	3006B49F3A30A80BB85074C279ACC7DF
SHA1:	728A7A867D13AD0034C29283939D94F0DF6C19DF
SHA-256:	F283B4C0AD4A902E1CB64201742CA4C5118F275E7B911A7DAFDA1EF01B825280
SHA-512:	E8FC5791892D7F08AF5A33462A11D39D29B5E86A62CBF135B12E71F2FCAAA48D40D5E3238F64E17A2F126BCFB9D70553A02D30DC60A89F1089B2C1E7465105DD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 73%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...Bu.c.....&.....X;.....@.....;....!.;. ..`.. .....8.....9.....8.....;.....8.(.....D.8.....text.....`..`.data....7.....7.....@. ...rdata.....8.....8.....@..@.pdata.....8.....8.....@..@.xdata.....8.....8.....@..@.bss....8....8.....idata.....8.....8.....@....CRT.... h.....8.....8.....@....tls.....9.....8.....@....rsrc.....9.....8.....@....reloc.....;.....Z;.....@..B..... .....

C:\Users\user\AppData\Local\Temp\aafg31.exe

Process:	C:\Users\user\AppData\Local\Temp\3C54.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	973312
Entropy (8bit):	4.572314384956297
Encrypted:	false
SSDEEP:	12288:5sJc/3ljJhGbZmEWh6dSs/1xsBwggGLXKPXPiXuHNHGb6bH/zx/GCLW/nh/X:5sMhVhC37ggG
MD5:	B4F79B3194235084A3EC85711EDFBD38
SHA1:	4E5DC4085DAFBE91F8FBE3265C49A9BF6E14E43D
SHA-256:	D425F18F931A8224C162FEE1804E5101BC538FE8E85C7A11D73D2BA4833ADDF4
SHA-512:	B22737BB7D80FC87D40B3762EB51B921B7AE1BA6BB3BA20F0E6940F5E91EB23DDBB44C9E8F8A7F9EE332542738CBF700688629EBA17E7D04190E5DB95A019964
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 33%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4.Z...Z..Z.iu....Z.iu....Z.iu....Z...[..Z.iu....Z.iu....Z.iu....Z.iu....Z.Rich. .Z.....PE..d...\..R.....".....t5.....@.....D.....`..... .....`/...p...'..... .....text..... ..`.data....B... ...:.....@....pdata...'...p...(...B.....@....idata...(.....*...j.....@..@.rsrc...`/.....0..... .....@..@.reloc..D.....@..B..... .....

C:\Users\user\AppData\Local\bowsakkdestx.txt

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	560
Entropy (8bit):	6.009613601911672
Encrypted:	false
SSDEEP:	12:YGJ68UiiMLwLR8AFq5I5WhsRtCV64uzR5W:YgJUFfFxg0cV/MI
MD5:	9252E3DCF847925C8080204C028EBAE6
SHA1:	498661D45D44EDED195FBB98AEC310D87BF1947E
SHA-256:	2ED806DEEF0185D3983A46422B07B33CB62FF04873066C7E315876C644B4D4D8
SHA-512:	71970EFCE4E86B1415696A792DC595F7E9993A587B34D4E000677B8C647A6CDE43845B7E1EBE3EE7F54D0937D2D42B4F8C3ED1C7F4468D2BF8392D57E3A625D3
Malicious:	false
Reputation:	unknown
Preview:	{"public_key":"-----BEGIN PUBLIC KEY-----\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzVVm4tu5iyZw13a\/GiU0\\nV5T6yum3k8oXJuPfu\ /dlDp5n6Tzk6N8vnuKpjC8lkV7xuMYgdtfQ4cWYKxUvBMa5\\nZoYlzVSlrIVedQM2wz2yOUQcOloagsxQEzv9Of3rNy2gF4dr82Kp8laqDk0c3hjz\\nmazDrTR\/jjRh NxY80qI9FZk8pFyou7p\/wowlaHHEiFkCdD2yrZBW1b8jmpuEPqdm\\nH+Nas4N51zRvyqkWCKO68bPnX70ZcR1zLiCfJNxJJ\/wx\/uRwZXCJW3Mhdz+bwMqd\\nhECMf f6Chw2XhPIKlGEHGhqCwRLO+yfVnjAF8Tu6hWIg7qhC0tx1sT2u6Xy02NLT\\ntQIDAQAB\\n-----END PUBLIC KEY-----\\n","id":"az8OAYewNgELvwQrvCQFNi 4j455hRwuI26KpqTgc"}

C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	802304
Entropy (8bit):	7.685061735084475
Encrypted:	false
SSDEEP:	24576:6nRTyItqh7DLUjjuiX+tR+WoXeAWG1qzz5E:8TZta/Uja7siAW
MD5:	6944FCA258A9009F9D3B7212CDB4874D
SHA1:	1E20555089B3D2B9E34B44422C8E6C3061E68F0E
SHA-256:	D34D06CCD3BA7877664E4769FF708D7C412EE5F43A76F2A2CE962C843CC5C35B
SHA-512:	A05299352297160D62FB91A75EC7D30E8C00CDAB97BFEF112429B0CED6041A3E6FB232686FF6A4080E9C98797B4D224792C6339600084DED4B12B0595575EDC
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...|.....|.....|...H...EX..k...b.....|...c...|...c...|...c...Rich b.....PE..L....4.a.....N...(&.....YN.....`....@.....0.....Q..d.....`0.... .....P1..@..... .....text...JL.....N..... ..`.data...DX$..`.....R.....@....rsrc.....p.....@..@.reloc...8...`0..:.....@..B..... ....

C:\Users\user\AppData\Roaming\07c6bc37dc5087\clip64.dll

Process:	C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.621829903792328
Encrypted:	false
SSDEEP:	3:qVoB3tUROb0b0qHXboAcMBXqWrKb0GkIlVLLPROZ/eIwcWWGu:q43tlkObRHXiMIWObtkII5LPROeIpfGu
MD5:	1B7C22A214949975556626D7217E9A39
SHA1:	D01C97E2944166ED23E47E4A62FF471AB8FA031F
SHA-256:	340C8464C2007CE3F80682E15DFAFA4180B641D53C14201B929906B7B0284D87
SHA-512:	BA64847CF1D4157D50ABE4F4A1E5C1996FE387C5808E2F758C7FB3213BFEFE1F3712D343F0C30A1681974984095465 4A70611D2250FD0F7B032429DB7AFD2CC5
Malicious:	false
Reputation:	unknown
Preview:	<html>..<head><title>404 Not Found</title></head>..<body>.. 404 Not Found ..<hr> nginx/1.18.0 (Ubuntu) ..</body>.. </html>..

C:\Users\user\AppData\Roaming\07c6bc37dc5087\cred64.dll

Process:	C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1074176
Entropy (8bit):	6.478034514486552
Encrypted:	false
SSDEEP:	24576:YVaH8jJPWhQnZzrZ+7xr1rZfVlTxd43v7t5m:2AhQnZzrZSxxZfVlUD
MD5:	16FD83A682162D6EDC119DC12C9990DC
SHA1:	4B5F38C78C8E5F1333989DA0912E945335F82C95
SHA-256:	36BE2F6CCCDF3EDC709E7DABCBE529D4F6390D3C624BA10FB471BD05D36060C8
SHA-512:	5AF414C95DB738D0A65FDD67F2FF3923C451EE68856237F55626586AAC14EFE62288F5B8D74A5FBF2EABA9E6A1689CEA89B856212A597AB12A3A4B0097E3F3A 5
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: C:\Users\user\AppData\Roaming\07c6bc37dc5087\cred64.dll, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Roaming\07c6bc37dc5087\cred64.dll, Author: Joe Security • Rule: OlympicDestroyer_1, Description: OlympicDestroyer Payload, Source: C:\Users\user\AppData\Roaming\07c6bc37dc5087\cred64.dll, Author: kevoreilly
Antivirus:	• Antivirus: ReversingLabs, Detection: 83%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sO..sO..sO..wN..sO..pN..sO..vNe.sO..vN..sO..wN..sO..pN.. sO..rN..sO..rOi.sON.zN..sON.sN..sON..O..sON.qN..sORich..sO.....PE..d....T.c....." .....H.....`..... `{..X....{.....h.....p.....p.....text..... ..`.rdata.....@..@.data....o.....6...|..... ....@....pdata.....@..@_RDATA.....J.....@..@.rsrc.....L.....@..@.reloc..h.....N.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe

Process:	C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build3.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9728
Entropy (8bit):	5.3362059272001
Encrypted:	false
SSDEEP:	192:9UEc8b6H1LE+4LoGgMatAJ2lzUw317NyEpvNHhqyo:9UUE1BYoGza/D3170kiyo
MD5:	9EAD10C08E72AE41921191F8DB39BC16
SHA1:	ABE3BCE01CD34AFC88E2C838173F8C2BD0090AE1
SHA-256:	8D7F0E6B6877BDFB9F4531AFAFD0451F7D17F0AC24E2F2427E9B4ECC5452B9F0
SHA-512:	AA35DBC59A3589DF2763E76A495CE5A9E62196628B4C1D098ADD38BD7F27C49EDF93A66FB8507FB746E37EE32932DA2460E440F241ABE1A5A279ABCC1E5FFE 4A
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Clipboard_Hijacker, Description: Yara detected Clipboard Hijacker, Source: C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe, Author: Joe Security • Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe, Author: unknown
Antivirus:	• Antivirus: ReversingLabs, Detection: 88%
Reputation:	unknown

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o.....o.....Rich.....PE..L.....a..... .....0....@.....`.....@.....:..<.....P.....9..8.....0..0.....text..... ..... ..`.rdata.....0.....@..@.data...`....@.....@....reloc.....P....."..... .....@..B..... ....

C:\Users\user\AppData\Roaming\ewgujdv

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	288768
Entropy (8bit):	6.584915706285476
Encrypted:	false
SSDEEP:	3072:tiaWGvA5BMvdYuAJ2qiGD0swth9Ewaf/s7htn5gYTtic7:t4GvAMdj40th7a3s7SYTtic
MD5:	7A8E3D000FBA0F5765B98E2D78EB9D12
SHA1:	2DFF944F970FAEF5C6FA92AC8FBE82C9251553F3
SHA-256:	13744BE5698FFDDC96D55415FDEEBDE4921ED199B4174251D83F1FD5B5A05C66
SHA-512:	1D56B0DD129D7A1C1E76B110F9CEE4C63D2F021BCDCACA53CD780CC5E6B6CAFD6CEBC70FB62198910CAE2E4E9EA083216611923C72A4120FCC30CA3894A08DA
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b.....PE..L...G..c.....~...."&.....YN.....@.....(.....d.....&.....(..... .....P1..@..... .....text....}.....~..... ..`.data...DX$.....@....rsrc.....&.....@..@.reloc...3....(..4...4.....@..B..... ....

C:\Users\user\AppData\Roaming\hwgujdv

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	289280
Entropy (8bit):	6.585305891932375
Encrypted:	false
SSDEEP:	3072:1nsNTcFBW0dKNogILXJ6WPLpjHysySMX3YpCUtn5grTtiFmAevZ:qNTcddpgInDtHMn3frTti9
MD5:	3D8207E1CE6762FF10DB118BEE3BD99B
SHA1:	82A02D6E00DE00074B48BA3CC76424A6EFE3E6AB
SHA-256:	C38267836DDE53953018C962A372E8E74153F97932418B682FC653ECFCB7BECE
SHA-512:	CA346B7FCD302A5D4AFBDCEB8D4A50F28D14068D9A72AD9960F647F19810D4936D0514A9ECD3FB2A14B87E7F82C0DF33AEEB02BFA64BEB394F5EB46FA6810D1A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 38%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...\|.....\|.....\|...H...EX..k...b.....\|...c...\|...c...\|...c...Rich b.....PE..L...e..c.....".....&.....YN.....@.....(.....d.....&.....(..... .....P1..@..... .....text...z..... ..`.data...DX$.....@....rsrc.....&.....@..@.reloc...3....(..4...6.....@..B..... ....

C:\Users\user\AppData\Roaming\hwgujdv:Zone.Identifier

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**

Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Desktop\CZQKSDDMWR.png

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.849718478245105
Encrypted:	false
SSDEEP:	24:ekjXaeaUX6GJpf7xkJGL+bwCFCCqdz2cQK575neVO57K9JgiJCFr4pBf/n0Xa/Q1:ewXaI6SEsCcCJcdAIEJgiJAG90Xa/UD
MD5:	80B888723A2D18278EAD53B06FDCCEBD
SHA1:	7EE1E787B9DC77807E9468BD108FC3BBB39ED20F
SHA-256:	4D67D7BE5A6B7B83A56F794E7AB1947E1B6EFBE5C3DFBFB1360C93EB723CA6E6
SHA-512:	2E0951A532C2A7C37F347BAC627215ACAE10BC737C1136D87818134ADC8055AB809307039698F48B08F64FE5C83B41BA9A5B3553A88ABD92423D138D21A4696E
Malicious:	**true**
Reputation:	unknown
Preview:	CZQKST.^$.....S..w[.W.&.s....k...d.1G.s..u..W....&......O;...e....fS....Pvt..D...YA;..V..t.#..}../kA\U.Ux}.v)...f..q.\$..a.X.9K..0....j.U&D...B...r.z.p.....v..o..]..@..g.p../.=.Z.!].T.)K.. ..}v....."9....4..!_^H.4.{.O,..".:,K..ZC.Y\|.W\...Q...=....<.z....;!... y.X...S...h.hg.....&.....w.[...'.x....<...)....v.ScV}^60..V(=F...*....s?..>.....[...JM..\.(.Z.t.....$..Fy...h4..Yj.....\...4 ....i..3iT.}...P/#.r.(I....-0.bl...=..S..r....M.:\.zA*..k..)W..j..0C..)..'.........I.k ....).%....f...n.}...L.....a...#84.&..U. @.t~..../..;.^.n..i.+.....I>.;...M.T..\....mzE@.I.YNC...N3.r.#Zh.. I.&.;..]E.e.A.(M .e...&.^k,W../.zk'.I?....s.#qEH..r.....1[..~.>ke'Y....BE.....M....o!#.eC..f.V[i...i|{."..]...S.....{?l.c=.P...".?f..."7.]..;.[...8..1G4.z...v.W..p.V(....Y..'.+.,..D{%<....\....ngnc ..k..$..<..C...mu.%!./..E...d...?}E.....|..~...H..>...1S)RU..A.(.~..B..9t*.j..I....K..b....T.#..T.....F....^I8.F...R.....]...b..e.Q.._.m.G.W8tkB.c.lQ..$...bG

C:\Users\user\Desktop\CZQKSDDMWR.png.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.849718478245105
Encrypted:	false
SSDEEP:	24:ekjXaeaUX6GJpf7xkJGL+bwCFCCqdz2cQK575neVO57K9JgiJCFr4pBf/n0Xa/Q1:ewXaI6SEsCcCJcdAIEJgiJAG90Xa/UD
MD5:	80B888723A2D18278EAD53B06FDCCEBD
SHA1:	7EE1E787B9DC77807E9468BD108FC3BBB39ED20F
SHA-256:	4D67D7BE5A6B7B83A56F794E7AB1947E1B6EFBE5C3DFBFB1360C93EB723CA6E6
SHA-512:	2E0951A532C2A7C37F347BAC627215ACAE10BC737C1136D87818134ADC8055AB809307039698F48B08F64FE5C83B41BA9A5B3553A88ABD92423D138D21A4696E
Malicious:	false
Reputation:	unknown
Preview:	CZQKST.^$.....S..w[.W.&.s....k...d.1G.s..u..W....&......O;...e....fS....Pvt..D...YA;..V..t.#..}../kA\U.Ux}.v)...f..q.\$..a.X.9K..0....j.U&D...B...r.z.p.....v..o..]..@..g.p../.=.Z.!].T.)K.. ..}v....."9....4..!_^H.4.{.O,..".:,K..ZC.Y\|.W\...Q...=....<.z....;!... y.X...S...h.hg.....&.....w.[...'.x....<...)....v.ScV}^60..V(=F...*....s?..>.....[...JM..\.(.Z.t.....$..Fy...h4..Yj.....\...4 ....i..3iT.}...P/#.r.(I....-0.bl...=..S..r....M.:\.zA*..k..)W..j..0C..)..'.........I.k ....).%....f...n.}...L.....a...#84.&..U. @.t~..../..;.^.n..i.+.....I>.;...M.T..\....mzE@.I.YNC...N3.r.#Zh.. I.&.;..]E.e.A.(M .e...&.^k,W../.zk'.I?....s.#qEH..r.....1[..~.>ke'Y....BE.....M....o!#.eC..f.V[i...i|{."..]...S.....{?l.c=.P...".?f..."7.]..;.[...8..1G4.z...v.W..p.V(....Y..'.+.,..D{%<....\....ngnc ..k..$..<..C...mu.%!./..E...d...?}E.....|..~...H..>...1S)RU..A.(.~..B..9t*.j..I....K..b....T.#..T.....F....^I8.F...R.....]...b..e.Q.._.m.G.W8tkB.c.lQ..$...bG

C:\Users\user\Desktop\GLTYDMDUST.mp3

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.858838390859525
Encrypted:	false
SSDEEP:	24:3y3l5QjWiby3yS9+A9zUkETmdv9iAG482muCh93NB7bD:i3lMa9P9okETmvDdo9dB/D
MD5:	F7C0A521155D3CD6393BA9E551917D2F
SHA1:	073C1B990B59024F480A2D3106CE7DF32B2552B6
SHA-256:	53D5B6B48B45B4589F68560B96C99E1243818803E21A614612C6EF69BCBEDDB7
SHA-512:	D2FD864776B351F7942619DC1C147EF9384F9C53455E0DF440661EDF205997B082E4D6D68762F1386DEF2F088BD62AD5DEE0F2ECB85E6C61967C3B10649E2EB
Malicious:	false
Reputation:	unknown
Preview:	GLTYD...q09....<.j..P.....Y.u~..i....g.....17...$.....s....& ....(<D.#...-...<.'9...".vn$..o..F .F.s..=..3Y.'.$.iJ.5.2...(.M[}...P....6.m.L..Q...pM...j.....0.).&...c.B..p/6..7...B6XB['9.6...G.... ..A..D.....qG.....53.[.bP...'Mc.y'..[.....rn..~4"....+I...~.....01_".pE..rj+@a....y....#k....Q.5.t$|]..YY=.D.,...hf2...N...I..J.d.<....)c....i.%.7..{<.|....ci.{..'3*..H..../....R..p.X.....D.'xM..M .V..n|.2Z...ia.R..Fv.&.....3f\.F.....5[i..O.R.-..eeSw.Tk...8..E..j..#h.t/@.'.^.$....#..;...\|.Z.J._.....U..&.'.[\|...@.(..xq.:....I.T.'T.>.R.uX..5Mv...=.....D....'.7R....]..F@F[T.....I....=.b.L;. ..L.m.....F\.C....[Z..9.....a.Yg..+...0j.'....e..P..b.1Hf..N.)=....W.e.....Q.u....).lx...b.G[..@.j..;...'.....~fg+..I.....\_..-.,..-\3K.X}.i4....h).....P.j.?.1jW$....,h.J$.g...$..A.M ...aax.. .Q...`YD...8_....}eVPK.]$W.7.O.^.....c.\j.5..4).z...n.e.TM.uD:.K.w._"..../..HC..K..z.. ...4.K..O.U.\..eY....&..N...d.n....JTj...H.....+..&v.D....

C:\Users\user\Desktop\GLTYDMDUST.mp3.vapo (copy)	
Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.858838390859525
Encrypted:	false
SSDEEP:	24:3y3l5QjWiby3yS9+A9zUkETmdv9iAG482muCh93NB7bD:i3lMa9P9okETmvDdo9dB/D
MD5:	F7C0A521155D3CD6393BA9E551917D2F
SHA1:	073C1B990B59024F480A2D3106CE7DF32B2552B6
SHA-256:	53D5B6B48B45B4589F68560B96C99E1243818803E21A614612C6EF69BCBEDDB7
SHA-512:	D2FD864776B351F7942619DC1C147EF9384F9C53455E0DF440661EDF205997B082E4D6D68762F1386DEF2F088BD62AD5DEE0F2ECB85E6C61967C3B10649E2EB
Malicious:	false
Reputation:	unknown
Preview:	GLTYD...q09....<.j..P.....Y.u~..i....g.....17...$.....s....& ....(<D.#...-...<.'9...".vn$..o..F .F.s..=..3Y.'.$.iJ.5.2...(.M[}...P....6.m.L..Q...pM...j.....0.).&...c.B..p/6..7...B6XB['9.6...G.... ..A..D.....qG.....53.[.bP...'Mc.y'..[.....rn..~4"....+I...~.....01_".pE..rj+@a....y....#k....Q.5.t$|]..YY=.D.,...hf2...N...I..J.d.<....)c....i.%.7..{<.|....ci.{..'3*..H..../....R..p.X.....D.'xM..M .V..n|.2Z...ia.R..Fv.&.....3f\.F.....5[i..O.R.-..eeSw.Tk...8..E..j..#h.t/@.'`.^.$....#..;...\|.Z.J._.....U..&.'.[\|...@.(..xq.:....I.T.'T.>.R.uX..5Mv...=.....D....'.7R....]..F@F[T.....I....=.b.L;. ..L.m.....F\.C....[Z..9.....a.Yg..+...0j.'....e..P..b.1Hf..N.)=....W.e.....Q.u....).lx...b.G[..@.j..;..'.....~fg+..!.....\_..-.,..-\3K.X}.i4....h).....P.j.?.1jW$....,h.J$.g...$..A.M ...aax.. .Q...`YD...8_....}eVPK.]$W.7.O.^.....c.\j.5..4).z...n.e.TM.uD:.K.w._"..../..HC..K..z.. ...4.K..O.U.\..eY....&..N...d.n....JTj...H.....+..&v.D....

C:\Users\user\Desktop\GLTYDMDUST.pdf	
Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.870393822177167
Encrypted:	false
SSDEEP:	24:xh4mCvPCx0uriZ2bOxs5YyDRu/ZiARVf3VnAb57fYIgUdbD:/4mCHCx0uUs5VIBzRVfFgfMUdD
MD5:	AD097AF44D2CBB48AECE31913B6FB9FE
SHA1:	6F92F50F8D0DAC425CC71DD0962EA57CB36A85DD
SHA-256:	367074A82414CB4B534370783B64E2CD69B12E465C952749DE183F49ECC03BC1
SHA-512:	5067E8749EB7A83F03AADA2C793E9674276FA09DD6A8894799BC3E3ED34C01564A6D868697C453FFC40274367ACECA837572D1EFD71AC8009645CEC4D37F7D 7
Malicious:	false
Reputation:	unknown
Preview:	GLTYD...>.9.I.3.....I.....Z_&.]@..J'....4n.r3..G....8/.q....J...s.ci`.6.AQ...D %...1..(..S\@f.....wI..X.....T.cJG..ZJ.K.....s.... 8.C.1..^*.~.....c..M{."J.E...4..F.J.Lp.Z.....1g_.. .&.s..d.K...3.y.@...c..F...^mx#.b..U.o.....;....'b.*..8 ..i.....d.....Z|3.....I..]..w.D.....s..$;_....m.+..=+..r.c..[.XD.t=.w....j....iK..Y5n...zce.L....TT.....k..M..?LB....\|Z....-...!...8^#o.}. ..lZ{...@)..t.e}.G8.^.V.KTApe/.,..ZE....t.V...$... ..X.....9...0w.....TQ...(.k.`...{...G,B.....k7.....>..y./%.f..j.]..E..}...45.....my.....[.....s.....|x...Z..?....Hv*..A5"x.:..Q.".u..@.u. ...7..W3..Qt%...V/!..a.k0.M..z.."y...q.....QD} f.LO..b..G.x+.8.t...~..@q..`.X...j.S..Tq.....F.nP~...O.I.q...}.8....&...]$`....Zc.'.'....<.....5A.a|..s.j.....4-WFUH9B..C*.."q../H"...q..3 r9.k.~W..y.02.M.....Uw...%e_Q.A....(....*h.}..H']*J ...../Y..i..'(..[.d.....r.z8?.Cf...oS9.....y..}.....ZX..i.1.Hd|qYp..8..I.w.....U.....

C:\Users\user\Desktop\GLTYDMDUST.pdf.vapo (copy)	
Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.870393822177167
Encrypted:	false
SSDEEP:	24:xh4mCvPCx0uriZ2bOxs5YyDRu/ZiARVf3VnAb57fYIgUdbD:/4mCHCx0uUs5VIBzRVfFgfMUdD
MD5:	AD097AF44D2CBB48AECE31913B6FB9FE
SHA1:	6F92F50F8D0DAC425CC71DD0962EA57CB36A85DD
SHA-256:	367074A82414CB4B534370783B64E2CD69B12E465C952749DE183F49ECC03BC1
SHA-512:	5067E8749EB7A83F03AADA2C793E9674276FA09DD6A8894799BC3E3ED34C01564A6D868697C453FFC40274367ACECA837572D1EFD71AC8009645CEC4D37F7D 7
Malicious:	false
Reputation:	unknown
Preview:	GLTYD...>.9.I.3.....I.....Z_&.]@..J'....4n.r3..G....8/.q....J...s.ci`.6.AQ...D %...1..(..S\@f.....wI..X.....T.cJG..ZJ.K.....s.... 8.C.1..^*.~.....c..M{."J.E...4..F.J.Lp.Z.....1g_.. .&.s..d.K...3.y.@...c..F...^mx#.b..U.o.....;....'b.*..8 ..i.....d.....Z|3.....I..]..w.D.....s..$;_....m.+..=+..r.c..[.XD.t=.w....j....iK..Y5n...zce.L....TT.....k..M..?LB....\|Z....-...!...8^#o.}. ..lZ{...@)..t.e}.G8.^.V.KTApe/.,..ZE....t.V...$... ..X.....9...0w.....TQ...(.k.`...{...G,B.....k7.....>..y./%.f..j.]..E..}...45.....my.....[.....s.....|x...Z..?....Hv*..A5"x.:..Q.".u..@.u. ...7..W3..Qt%...V/!..a.k0.M..z.."y...q.....QD} f.LO..b..G.x+.8.t...~..@q..`.X...j.S..Tq.....F.nP~...O.I.q...}.8....&...]$`....Zc.'.'....<.....5A.a|..s.j.....4-WFUH9B..C*.."q../H"...q..3 r9.k.~W..y.02.M.....Uw...%e_Q.A....(....*h.}..H']*J ...../Y..i..'(..[.d.....r.z8?.Cf...oS9.....y..}.....ZX..i.1.Hd|qYp..8..I.w.....U.....

C:\Users\user\Desktop\GLTYDMDUST.xlsx	
Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.856079400934414
Encrypted:	false
SSDEEP:	24:niXk52wiDrzc+SSTYqOUKNDD2Y98mp9LK50Gp9eKRamxyB2aheP5vhKmm6mkybD:niXYiD08WUKNDCY98mp9KSGTeK88ahc2
MD5:	3CEA4C1502F0D6EE0DFD5B465DE0F718
SHA1:	04E287E9D3B7E72C8CD6FA1DBB27E846B6E0ACAB
SHA-256:	E771DC120F3BB48BA77BC0F8B8D07769265635D277EF085BB7632DDC1AC12A06
SHA-512:	F2D8609AC8E8478C6787F73BC98E2054D0BD9D848F4E28F1E0DB6173D528DA35BD00B7BD39CD5F8AC227566493C8A305545F7E0F3D4B3639136F49E1576C249
Malicious:	false
Reputation:	unknown
Preview:	GLTYDVD..W.w.F%/6Z...&$z....P@........".....H.f./...V.....\|G.gB7C.R..M.<.../..p.=..'..d8n2\|4.....q...j...c\|..).m.O.cr..c.....ig)....~A..y..x.Kz..@...rb.."(i....EW}.....K...\|....J.....xO M.N+#Q\|.....Vg..)...........,..a.....m.!...m.Vg..X.=hl...E>.X.Ke..H'....$.K..._..57v<.o.....3F...jH.:..o...O..&.7.....P...../....l;...B.v....vy..J.BN@..n...'dm.._.~w.m.Z.Pq.....Z.j\.w^. {....q.OQ....-...z.O.....f...=..IBl..I.48....(..I\.<#.%.8;...3^51.....N(..[...}..pmk....b.+J.yE~...^.m.w5...?...c+M.|[].P...}.N.B.F.....-qv^.....F...i.....}.I...U?u...jcq..Q.[.....c.."E... cU...jNa.g...s.s..I.....{_..`...y.@._.....q..._.....K2..z.9&...<..Mn.F.i.W..6r.....$..n.S\.....ss.~.....,U..0....&."..I.f{W..A!.^..6.S./...v..i)..7P....T)..._$A.....K..T.!...y.G. .#...v.....D..X....u|x.8f.nh3..JO.<.X.S.C.[WCS..Kc..N.T"h.9....M.J..-H.5....,..2.s.6...:i`,.ud0.o.v.C.D.B..]j...g.Wq.....$..Iz.....Dw.D.....

C:\Users\user\Desktop\GLTYDMDUST.xlsx.vapo (copy)	
Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.856079400934414
Encrypted:	false
SSDEEP:	24:niXk52wiDrzc+SSTYqOUKNDD2Y98mp9LK50Gp9eKRamxyB2aheP5vhKmm6mkybD:niXYiD08WUKNDCY98mp9KSGTeK88ahc2
MD5:	3CEA4C1502F0D6EE0DFD5B465DE0F718
SHA1:	04E287E9D3B7E72C8CD6FA1DBB27E846B6E0ACAB
SHA-256:	E771DC120F3BB48BA77BC0F8B8D07769265635D277EF085BB7632DDC1AC12A06
SHA-512:	F2D8609AC8E8478C6787F73BC98E2054D0BD9D848F4E28F1E0DB6173D528DA35BD00B7BD39CD5F8AC227566493C8A305545F7E0F3D4B3639136F49E1576C249
Malicious:	false
Reputation:	unknown
Preview:	GLTYDVD..W.w.F%/6Z...&$z....P@........".....H.f./...V.....\|G.gB7C.R..M.<.../..p.=..'..d8n2\|4.....q...j...c\|..).m.O.cr..c.....ig)....~A..y..x.Kz..@...rb.."(i....EW}.....K...\|....J.....xO M.N+#Q\|.....Vg..)...........,..a.....m.!...m.Vg..X.=hl...E>.X.Ke..H'....$.K..._..57v<.o.....3F...jH.:..o...O..&.7.....P...../....l;...B.v....vy..J.BN@..n...'dm.._.~w.m.Z.Pq.....Z.j\.w^. {....q.OQ....-...z.O.....f...=..IBl..I.48....(..I\.<#.%.8;...3^51.....N(..[...}..pmk....b.+J.yE~...^.m.w5...?...c+M.|[].P...}.N.B.F.....-qv^.....F...i.....}.I...U?u...jcq..Q.[.....c.."E... cU...jNa.g...s.s..I.....{_..`...y.@._.....q..._.....K2..z.9&...<..Mn.F.i.W..6r.....$..n.S\.....ss.~.....,U..0....&."..I.f{W..A!.^..6.S./...v..i)..7P....T)..._$A.....K..T.!...y.G. .#...v.....D..X....u|x.8f.nh3..JO.<.X.S.C.[WCS..Kc..N.T"h.9....M.J..-H.5....,..2.s.6...:i`,.ud0.o.v.C.D.B..]j...g.Wq.....$..Iz.....Dw.D.....

C:\Users\user\Desktop\GNLQNHOLWB.mp3	
Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.8483102131416524
Encrypted:	false
SSDEEP:	24:ZecFoShyYCsIX0hUP4yLHY5bXaYSGKEeYQVxRI2ckAJztuxbD:ZxGSsYCsLhUjoHSbWQVxRI2ck6ZMD
MD5:	94CEA18659A3DB14A08D113EE33C9DC3
SHA1:	C60D7FC52E907AE42AFD367B8FD011C99ED23366
SHA-256:	3586F2EB7576FCB0DFD09679267BAE1C0EAA94E4982C72CD470F971C67BE7AB6
SHA-512:	F44F97FF9EB55EBF656B73F3F2C26310E827D4C029E18B16620791EF9E3F2EF267368392A6CA6B8A964140026712A646D30AC872B6A4EFED3E9CA2B7582321C7
Malicious:	false
Reputation:	unknown
Preview:	GNLQNE..V.?I*}6....3..S.eg..z.6..w.X{1....6...[.....1".....Q.....|,.&.M.....v..kE.[.8.+...2...W.f%..^....0e.;~..,U>I.../.....-_i..`..x*....n.8G;...T...w..SI...AI....Y....NY../..]..>..=.. .o..g.....,...._\..v8.s.B.9.....i,.....`..I.pW+..rx&Ax.%s.g...+)H(..I\..;\.tL..S..H.."g.2.B..J....V.....?..w.....Su=.S...&..x`.}....1.....'..|.!<.p.F.:.c4.....|.....%...?..G.d.A7H?o...*Atg.. ;G...|....i>.....he.9.8....:.....>E._.fh...=y.>.g|.2....Vm....jNK.?IOVI....[.qA^...!...@...E.b..Z...(.(..J..:.5..].eT].Y._..V.@.s.....u8q.eF#."..w...B...-.....L....o..c.}.....(.N#...S?".@..j...k.. .%E.5~.+.hK.kO.....F..j.S.....MT 2.<.....|,. j#...r.v.x..m..[.Z?.W..H3G._#5f.G...V.n....[5...._./,.....,..H.%]..%(^,.kRf.....=.P.c..aS..G.]"..p..8.h..#..\.3..7s....8LW.....)..z..\Z ....gm...9y.....,5..D<..."...'.=z..p.6.....E.....#..}..K.L.<..}.Tm..U|.!.\.w...fDq. ..Y....U.,..7.w7/8..B.7).V..PQT....8.....@.w.4>.....?.

C:\Users\user\Desktop\GNLQNHOLWB.mp3.vapo (copy)	
Process:	C:\Users\user\AppData\Local\Temp\D804.exe

File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.8483102131416524
Encrypted:	false
SSDEEP:	24:ZecFoShyYCsIX0hUP4yLHY5bXaYSGKEeYQVxRI2ckAJztuxbD:ZxGSsYCsLhUjoHSbWQVxRI2ck6ZMD
MD5:	94CEA18659A3DB14A08D113EE33C9DC3
SHA1:	C60D7FC52E907AE42AFD367B8FD011C99ED23366
SHA-256:	3586F2EB7576FCB0DFD09679267BAE1C0EAA94E4982C72CD470F971C67BE7AB6
SHA-512:	F44F97FF9EB55EBF656B73F3F2C26310E827D4C029E18B16620791EF9E3F2EF267368392A6CA6B8A964140026712A646D30AC872B6A4EFED3E9CA2B7582321C7
Malicious:	false
Reputation:	unknown
Preview:	GNLQNE..V.?I*}6....3..S.eg..z.6..w.X{1....6...[.....1"......Q.....|,.&.M.....v..kE.[.8.+...2...W.f%..^....0e.;~..,U>I../.....-_i..`..x*....n.8G;...T...w..SI...AI....Y....NY../..]..>..=.. .o..g.....,....._\..v8.s.B.9.....i,.....`..!.pW+..rx&Ax.%s.g...+)H(..!\..;\.tL..S..H.."g.2.B.J....V.....?..w.....Su=.S...&..x`.}....1....'..|.!<.p.F.:.c4.....|.....%...?..G.d.A7H?o...*Atg.. ;G...|....i>.....he.9.8....:.....>E._.fh...=y.>.g|.2....Vm....jNK.?lOVI....[.qA^...!...@...E.b..Z...(.(..J..:.5..].eT].Y._...V.@.s.....u8q.eF#."..w...B...-.....L....o..c.}.....(.N#...S?".@..j...k.. .%E.5~.+.hK.kO.....F..j.S.....MT 2.<.....|,. j#...r.v.x..m..[.Z?.W..H3G._#5f.G...V.n....[5...._./,.....,..H.%]..%(^,.kRf.....=.P.c..aS..G.]"..p..8.h..#..\.3..7s....8LW.....)..z..\Z ....gm...9y.....,5..D<..."....'.=z..p.6.....E.....#..}..K.L.<..}.Tm..U|.!.\.w...fDq. ..Y....U.,..7.w7/8..B.7).V..PQT....8.....@.w.4>.....?.

C:\Users\user\Desktop\HMPPSXQPQV.png

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.858829878894281
Encrypted:	false
SSDEEP:	24:tIRgimxkoBiPNKqXWv9kcGBCJySHVuXZZzlgmT/gOAVNrtC5kytOPObD:tIqimxkRKupeXYZZzlgvyisD
MD5:	7F053371DFF62D82119164F040B6C9E9
SHA1:	14A0279F63A9F7EEB36ADCEB8717EDAF933EED33
SHA-256:	C839868C8A1FAE239DA80B158C78F0F3024035BE864BA17B5C1A3EBE95664FD6
SHA-512:	D644388F401F3C9B899B01DD174062DDBC7A2471BE147AE4A31A0B610CE06C57804DC8F4C88C3A66D2BAAA5817959054C069EA8646AA4F190D7513037545F50
Malicious:	**true**
Reputation:	unknown
Preview:	HMPPS.. *....H.`.\.0....`.OB.q[O.....Z.'.3^.6v.Sc~.y.^..q .FD1....Pm..!.He....v...Z7..)@f4h...a.....w.../...mM.....v.....f..\.4..9.9vY!L..JZ&w.1rt...c.....\b&Vm...^f*..(...@...h'...;.^%.. .]...TW..<(x.X ....E..u.+4.....X..$_...:.0.`.n.....w....o. .Bu].....2V...bR..w.lf.fE...iY..;.J?X..+B.K7..\.w.q.....,....#.>o.e.O.....Nj!{Y...W;q...sz.?....@.a.cS.../.V.L../.\E%..q.e Go..T.....*.....V.T..AU..]....MJ...U_.^.Z&.....z..L0.....^.SAt.\|q....Sq.B._...s.O.&Bv?...^....v...?.....-...w.....o:/T+>.h.&.y.7.Aj.0._.O.....w...{.0$n^..l.Q..-M.O.m.!&"Y.u.Y.2OF.] {.. [.Fg.8>A.w.T.....N..U z.i.:..@...S....D....M..>...M..@&T~.(...../.]..J.\g2..+.bp....?.....jX.."0...S..`...[#.I{./.zd.....9#.;..... E.....#.I..<=...`.{.cLb..z..7.)...F.k>...w.....f.C...?..g... (...U.,.....-....Vf....R;.m...\SE.y.....)w#%.G.....K.\b.. ....@.>.VIOg.J.;.S.~.....A....W..~~.M{j...;.....K..].2.....?.....P..u6..@:.rm_L.P.QND...%..y..^@

C:\Users\user\Desktop\HMPPSXQPQV.png.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.858829878894281
Encrypted:	false
SSDEEP:	24:tIRgimxkoBiPNKqXWv9kcGBCJySHVuXZZzlgmT/gOAVNrtC5kytOPObD:tIqimxkRKupeXYZZzlgvyisD
MD5:	7F053371DFF62D82119164F040B6C9E9
SHA1:	14A0279F63A9F7EEB36ADCEB8717EDAF933EED33
SHA-256:	C839868C8A1FAE239DA80B158C78F0F3024035BE864BA17B5C1A3EBE95664FD6
SHA-512:	D644388F401F3C9B899B01DD174062DDBC7A2471BE147AE4A31A0B610CE06C57804DC8F4C88C3A66D2BAAA5817959054C069EA8646AA4F190D7513037545F50
Malicious:	false
Reputation:	unknown
Preview:	HMPPS.. *....H.`.\.0....`.OB.q[O.....Z.'.3^.6v.Sc~.y.^..q .FD1....Pm..!.He....v...Z7..)@f4h...a.....w.../...mM.....v.....f..\.4..9.9vY!L..JZ&w.1rt...c.....\b&Vm...^f*..(...@...h'...;.^%.. .]...TW..<(x.X ....E..u.+4.....X..$_...:.0.`.n.....w....o. .Bu].....2V...bR..w.lf.fE...iY..;.J?X..+B.K7..\.w.q.....,....#.>o.e.O.....Nj!{Y...W;q...sz.?....@.a.cS.../.V.L../.\E%..q.e Go..T.....*.....V.T..AU..]....MJ...U_.^.Z&.....z..L0.....^.SAt.\|q....Sq.B._...s.O.&Bv?...^....v...?.....-...w.....o:/T+>.h.&.y.7.Aj.0._.O.....w...{.0$n^..l.Q..-M.O.m.!&"Y.u.Y.2OF.] {.. [.Fg.8>A.w.T.....N..U z.i.:..@...S....D....M..>...M..@&T~.(...../.]..J.\g2..+.bp....?.....jX.."0...S..`...[#.I{./.zd.....9#.;..... E.....#.I..<=...`.{.cLb..z..7.)...F.k>...w.....f.C...?..g... (...U.,.....-....Vf....R;.m...\SE.y.....)w#%.G.....K.\b.. ....@.>.VIOg.J.;.S.~.....A....W..~~.M{j...;.....K..].2.....?.....P..u6..@:.rm_L.P.QND...%..y..^@

C:\Users\user\Desktop\HQJBRDYKDE.jpg

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data

Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.848466650261886
Encrypted:	false
SSDEEP:	24:x/yaK9IcgWn0QdU8VDdWV2BX3esqtuwL67TcaTrvER756gbravkz2juPgwB2DIO4:x/yaKUDG3zHV3WLOlT8756gf70u4woDO
MD5:	D88517C21D71608B72F880E2F995CE23
SHA1:	4A25213AB601CAF49C1ABD802FA28A489CCE80E7
SHA-256:	1A27D850C6DFC356929F75E104FD71143007C2F869CCACAB66D9E6464FBB2354
SHA-512:	E29795E1440855E48FD0D14E291EC4986179E9507BC589471A9DD81F23E4CB208D0C8257FF63CA67B5123904730700CCF59AB9661E8B7B409F12B7F2A8F0EC97
Malicious:	false
Reputation:	unknown
Preview:	HQJBR.Q...@$K.q'u.G;.ICN2..5..W..8.....3..\|E6C.n.B.n..@...O.....r..n....a...h.F....h.iA...{..1/...6..J5..f.."Q\a.k0;;.....%.....z...d,"..@.z&.0.....e(y.6q....4*..o..ua.H..(o.m..L.2..q.. 0k.\|.&y...,..u.`.....s..&..K.%8k\|N...y'.....-Ah.....T... .E..4..u.....\.R.;e.B.q].....D.'.....#.0Pu.*r..D.....L...Cg.G.jr,]Ve9.KY.....mxB....!q@...*%.\.k.V.(%..R.?.\...m....B.-.-.. %PuB....v...a..O...k.jU.$fF&.....-P.j.(_..M..,?.....c..r.a.....rq:...lZ"..X.....0..#..(..K.....$..w.c..u...a(k....2;...|...b..O..9t:.6Y.J....g..$8^...w.r.....`..E.b;\|.....M.Fq.o...!=.W..!l P..!9.....d\|U>.e.?..]....*.,..../'.U...%..=<..GR.,\|(.t.H.....b..\|.zkk..<...5..m..U....F.^.....J.$D.?,.3..\..D..u.+|#...NryR.....{&2.f.-7-..W....|.....Y.=o"..Z...)V...[..J+.W....NS.$...c\.r..T.W.$... .B.....4...z.L.a.[_...(n..!-...Z%..W...e*.7..{*.5..../.p..n.IM.(...P..`.....$.so.<.Fj2l...X.'.....0.z$Gd.....\]..p....\.GH.....Oe.EY..<+..7`h.}.f."........9...m.C..6.Y

C:\Users\user\Desktop\HQJBRDYKDE.jpg.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.848466650261886
Encrypted:	false
SSDEEP:	24:x/yaK9IcgWn0QdU8VDdWV2BX3esqtuwL67TcaTrvER756gbravkz2juPgwB2DIO4:x/yaKUDG3zHV3WLOlT8756gf70u4woDO
MD5:	D88517C21D71608B72F880E2F995CE23
SHA1:	4A25213AB601CAF49C1ABD802FA28A489CCE80E7
SHA-256:	1A27D850C6DFC356929F75E104FD71143007C2F869CCACAB66D9E6464FBB2354
SHA-512:	E29795E1440855E48FD0D14E291EC4986179E9507BC589471A9DD81F23E4CB208D0C8257FF63CA67B5123904730700CCF59AB9661E8B7B409F12B7F2A8F0EC97
Malicious:	false
Reputation:	unknown
Preview:	HQJBR.Q...@$K.q'u.G;.ICN2..5..W..8.....3..\|E6C.n.B.n..@...O.....r..n....a...h.F....h.iA...{..1/...6..J5..f.."Q\a.k0;;.....%.....z...d,"..@.z&.0.....e(y.6q....4*..o..ua.H..(o.m..L.2..q.. 0k.\|.&y...,..u.`.....s..&..K.%8k\|N...y'.....-Ah.....T... .E..4..u.....\.R.;e.B.q].....D.'.....#.0Pu.*r..D.....L...Cg.G.jr,]Ve9.KY.....mxB....!q@...*%.\.k.V.(%..R.?.\...m....B.-.-.. %PuB....v...a..O...k.jU.$fF&.....-P.j.(_..M..,?.....c..r.a.....rq:...lZ"..X.....0..#..(..K.....$..w.c..u...a(k....2;...|...b..O..9t:.6Y.J....g..$8^...w.r.....`..E.b;\|.....M.Fq.o...!=.W..!l P..!9.....d\|U>.e.?..]....*.,..../'.U...%..=<..GR.,\|(.t.H.....b..\|.zkk..<...5..m..U....F.^.....J.$D.?,.3..\..D..u.+|#...NryR.....{&2.f.-7-..W....|.....Y.=o"..Z...)V...[..J+.W....NS.$...c\.r..T.W.$... .B.....4...z.L.a.[_...(n..!-...Z%..W...e*.7..{*.5..../.p..n.IM.(...P..`.....$.so.<.Fj2l...X.'.....0.z$Gd.....\]..p....\.GH.....Oe.EY..<+..7`h.}.f."........9...m.C..6.Y

C:\Users\user\Desktop\LFOPODGVOH.jpg

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.822811184260018
Encrypted:	false
SSDEEP:	24:y4dWOKlpjkUrwXRdbdelWYR3vEfCeXjtnubPToIJdwSvcPrJoUQEIZo7bD:yfO/tkUKdbaWi3vE1jdEPzB0PrwEGED
MD5:	7A0C7E6D65962EFB7F74D1C8E9224519
SHA1:	2778C98C36E47AD89F5E52E11DDFD88B78AAF5F0
SHA-256:	59D6FFAD1474FD2D62F8CC6B102690B0CDE2C071255DF11A0295EEE49ABED6AF
SHA-512:	40E6EC378E85330E57094A93E10FB1B6A19FE661119EADFEDBB7A1C33A5C1AFB293129339E0F41C3030AC129D4D2448C6EFAB3497DA621E44FE5BFDE3743E527
Malicious:	false
Reputation:	unknown
Preview:	LFOPOW.>.....z.r.M.}04....,*..8.1pQ.....u..(w....C.....i%.I........O$4DW\..2.v...Kc...iqeb\|..-...0.....jUo/.../3z..\...G...n}7q.....Up.2..?.c.W....I.SL6.J...`~QaY..!9....an..K...DAoJ}..... ....$qWK.yh.U.....Y.u..T"..m.....}..8"..i'./.?...w..D..K.._.C.....4.....Hm.....~@|...=..WK.n..Rw.....F\.$.?.y.B.6.....z\|.3I.Ixpe..#e.....~.K.-W....7}X.87.....G[.H.P.O%..A.....r5....I ..@..P..P!6+..j...x.S..=..lJ6T.xzEQ...Y.j.J.'...I.0....4A.}.c}E.....n.K.x;...Nz..Aa...6..L.;@O(..v.a\...V\Mz..\.4<.....:...Ys)U1V...x...]..u:. '.....IF%(`....H...!.p._q.....\.....w4....N.I7).. Y&..t..8D\|....G.S}.J.(.cn..5..H..I.7?.H.!q..E....8oy.sr(....<.CC.g.~...0.B.j.F.I...ap..VY.....K..-..E..8.....F...A...;1.....e.$o...0.tcU&_Iv.....|P.iH..>^.|.B.b.N._..X...?....d...W..XKz.e.? ..0....`0..QJ....jp.r.....jV.P..g.6.(K .hl..z.....-...?L|.F..|."....&D..A..{.D...[_.T>.....(u.\.....^...H-.....u..jo..C....[f.r.X.|...{..g.....u.^.g5t=.0..... ..0O ./..r

C:\Users\user\Desktop\LFOPODGVOH.jpg.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360

Entropy (8bit):	7.822811184260018
Encrypted:	false
SSDEEP:	24:y4dWOKIpjkUrwXRdbdelWYR3vEfCeXjtnubPToIJdwSvcPrJoUQEIZo7bD:yfO/tkUKdbaWi3vE1jdEPzB0PrwEGED
MD5:	7A0C7E6D65962EFB7F74D1C8E9224519
SHA1:	2778C98C36E47AD89F5E52E11DDFD88B78AAF5F0
SHA-256:	59D6FFAD1474FD2D62F8CC6B102690B0CDE2C071255DF11A0295EEE49ABED6AF
SHA-512:	40E6EC378E85330E57094A93E10FB1B6A19FE661119EADFEDBB7A1C33A5C1AFB293129339E0F41C3030AC129D4D2448C6EFAB3497DA621E44FE5BFDE3743E527
Malicious:	false
Reputation:	unknown
Preview:	LFOPOW.>.....z.r.M.}04....,*..8.1pQ.....u..(w....C.....i%.I.....O$4DW\..2.v...Kc...iqeb\|..-...0.....jUo/.../3z..\...G...n}7q.....Up.2..?.c.W....I.SL6.J...`~QaY..!9....an..K...DAoJ}.....$qWK.yh.U.....Y.u..T"..m.....}..8"..i'./.?...w..D..K.._.C.....4.....Hm.....~@|...=..WK.n..Rw.....F\.$.?.y.B.6.....z\|.3I.lxpe..#e.....~.K.-W....7}X.87.....G[.H.P.O%..A.....r5....I..@..P..P!6+..j...x.S..=..lJ6T.xzEQ...Y.j.J.'...I.0....4A.}.c}E.....n.K.x;...Nz..Aa...6..L.;@O(..v.a\...V\Mz..\.4<.....:...Ys)U1V...x...]..u:. '.....IF%(`....H...!.p.._q.....\.....w4....N.I7)..Y&..t..8D\|....G.S}.J.(.cn..5..H..I.7?.H.!q..E....8oy.sr(....<.CC.g.~...0.B.j.F.I...ap..VY.....K..-..E..8.....F...A..;1.....e.$o...0.tcU&_Iv.....|P.iH..>^.|.B.b.N._..X...?....d...W..XKz.e.?..0....`0..QJ....jp.r.....jV.P..g.6.(K .hI..z.....-...?L|.F..|."....&D..A..{.D...[_.T>.....(u.\....^...H-.....u..jo..C....[f.r.X.|...{..g.....u.^.g5t=.0..... ..0O ./..r

C:\Users\user\Desktop\LFOPODGVOH.xlsx

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.868850440755465
Encrypted:	false
SSDEEP:	24:AdSy/hos9+1BLZjBGlaFfA0BWJ11UH2KjRbiIDsTiy1l2VijwZjG7sbD:UCs9+1BLY4/C1UWK4BH1l2Vlx5D
MD5:	CA35043CCD05D3CDCCD5B4AD8E2E060F
SHA1:	D1D5151101D8A0B6AC9CA162AE32F6422408DAEA
SHA-256:	34C9187055110A0B07DF31212083B88093494E8571324744F2F90E25C4182966
SHA-512:	740E19B42056C5F8422B1005D2A0DEB5C352BB5BEF71DF203C1411808C2301D85B2F19814B0FE9BADF1F5AA7250A788A2537C1511066D24C07C09007B91AB9FE
Malicious:	false
Reputation:	unknown
Preview:	LFOPO.`..%..w....7.....Z)...+b.A....0T...p*h...{(..R...w.H.94.C.Xq..~...,.>d.k;...d.|.,.,...a...D..e..\..U...@N..sK.y....9.....m..1..a..FS....6.q.....M0...P`H...w.ae.....^.f@..~.+O...-..'Q.A.K.....%.n.u.....g..!.....$.. ./.....%3..(.U..]....=..E..v..\|.I!/....[d..\.....L.=.....\|.....1..i.JC.JGA....=f .....`...}..)...A$Q&....I.sZ.....,I4....2.q...?[.F.2t..b{.....w.d...Y].?...z':....<...8MGe...1...hY.X...s.2m..$:.P0`.}..a.1}.g...G..36Z..+.I.\.\|.=%..C....V!.3....E..~:._mj~....{.....K..5...;.@#...P.d.O...$...6F....fC...E.f4~.....Mu.._|.....3,I.y.....T.....jf....b....v.._..zT..q.sG...A-.7..Eq>..V.M7.H.....y..).1..0i.....W).`vtq.a..<`}r.r_07.[..Ds.Z....~.JyP .v.....Y.h.....4Di....^.#V`2....K..\.?.....g.....V..I....B..Z..!...<.G^.Z.C.....F.;.N.`[!e....@..C...B..6.9..XU.c.H..n1..7.z.....{.[...o..eG]../P(.1. .... !..T.^..:.i.I.kl=.....n....XWF...BSO..2{.B..)...E.e....M"..P...a.q;Z..../>.\.M..).{0.3..x.

C:\Users\user\Desktop\LFOPODGVOH.xlsx.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.868850440755465
Encrypted:	false
SSDEEP:	24:AdSy/hos9+1BLZjBGlaFfA0BWJ11UH2KjRbiIDsTiy1l2VijwZjG7sbD:UCs9+1BLY4/C1UWK4BH1l2Vlx5D
MD5:	CA35043CCD05D3CDCCD5B4AD8E2E060F
SHA1:	D1D5151101D8A0B6AC9CA162AE32F6422408DAEA
SHA-256:	34C9187055110A0B07DF31212083B88093494E8571324744F2F90E25C4182966
SHA-512:	740E19B42056C5F8422B1005D2A0DEB5C352BB5BEF71DF203C1411808C2301D85B2F19814B0FE9BADF1F5AA7250A788A2537C1511066D24C07C09007B91AB9FE
Malicious:	false
Reputation:	unknown
Preview:	LFOPO.`..%..w....7.....Z)...+b.A....0T...p*h...{(..R...w.H.94.C.Xq..~...,.>d.k;...d.|.,.,...a...D..e..\..U...@N..sK.y....9.....m..1..a..FS....6.q.....M0...P`H...w.ae.....^.f@..~.+O...-..'Q.A.K.....%.n.u.....g..!.....$.. ./.....%3..(.U..]....=..E..v..\|.I!/....[d..\.....L.=.....\|.....1..i.JC.JGA....=f .....`...}..)...A$Q&....I.sZ.....,I4....2.q...?[.F.2t..b{.....w.d...Y].?...z':....<...8MGe...1...hY.X...s.2m..$:.P0`.}..a.1}.g...G..36Z..+.I.\.\|.=%..C....V!.3....E..~:._mj~....{.....K..5...;.@#...P.d.O...$...6F....fC...E.f4~.....Mu.._|.....3,I.y.....T.....jf....b....v.._..zT..q.sG...A-.7..Eq>..V.M7.H.....y..).1..0i.....W).`vtq.a..<`}r.r_07.[..Ds.Z....~.JyP .v.....Y.h.....4Di....^.#V`2....K..\.?.....g.....V..I....B..Z..!...<.G^.Z.C.....F.;.N.`[!e....@..C...B..6.9..XU.c.H..n1..7.z.....{.[...o..eG]../P(.1. .... !..T.^..:.i.I.kl=.....n....XWF...BSO..2{.B..)...E.e....M"..P...a.q;Z..../>.\.M..).{0.3..x.

C:\Users\user\Desktop\LHEPQPGEWF.mp3

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.8601419602885585
Encrypted:	false

SSDEEP:	24:9b+wY9JFwd/Ta2PpVRjYfUIP7/cDqcqDZtFjOuP7Lj3w6f0b2vuWWNLaK89bD:9kbi5TbxknDKqjvFjOuP7Lj3E29f3D
MD5:	7DE9D9D42F41CEA67DB6C07FF2284B4D
SHA1:	A8F0594CD749540EB69A5D9B1A871F03FE44F6B5
SHA-256:	BA07BADA6F282D3A0EB7CEF900D5E49C5D30675B31681AAAB21CF6DDCB2889CE
SHA-512:	8D748EE73E773170B8FE011FE9CE3D9A8DF5A3A15191616382B57EF63217927CFFC0DDCC37274E0D3510A74F507B3A876863426CC1A83854B46582D1E0822178
Malicious:	false
Reputation:	unknown
Preview:	LHEPQ|..K..h_..d<...L.(.K.vc.z]..Z5...B..(..6..b....v.j......g....66.B.3./%U`...zI.....I...c...v...S.....6.G....+.`.H}....v....<.....U.....Jx....].....E....[..{Wg~.KT.....K.%x.....~|..c.F....jd. ...w.....=.+.$,H.....e..ai...pt...G...Z..2.I.O.$.%.]...;08l.ESN..Q.[gu..H...@z....N.`Z...M..s7.}.....4.`;e..\.(.r.M..t.....(U...f.U\.I....1....."p..xv5+...U.*.h0..S..5.U.m.e.f0.n2V&1.-]..M.t.@.kg..b.n;.l@.0K.W>.!BX.,.."...=.dG..Gt....p...h'.'...v[q...H..^>.Y.....Nr.D..$T.....y.d.=.._mN.....4e...S....^....).h"K...Z.....}....<Ap.~....d...2..!...n. .MJ..M..@.e.i.=.. .X...qpw+.J0.C.q...o.n..\..-W.c.$vP;0..EA...J.L.....C.1...E.D7'|:...=P.3.HB..K1..A$./S...,.X....t..t.2..E.w.c..._..Vf.Akd..1\..%.q...gW.h..X'.-...f$x'..KV..!...5tx$.z.e.&.(w.wC.... ..m.!yA.\.Ff.~?..}@B.j.....A...B....-.zX..RL..b...5O9.....Ta....b.[\|k....h..2....K3..k...-&.'..^....:...;F^..!..'XL.ID..Q!$i.[.G.<....."K...x.m.A>..1U..y..R.;F}c.).EU.&.....0.[+.

C:\Users\user\Desktop\LHEPQPGEWF.mp3.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.8601419602885585
Encrypted:	false
SSDEEP:	24:9b+wY9JFwd/Ta2PpVRjYfUIP7/cDqcqDZtFjOuP7Lj3w6f0b2vuWWNLaK89bD:9kbi5TbxknDKqjvFjOuP7Lj3E29f3D
MD5:	7DE9D9D42F41CEA67DB6C07FF2284B4D
SHA1:	A8F0594CD749540EB69A5D9B1A871F03FE44F6B5
SHA-256:	BA07BADA6F282D3A0EB7CEF900D5E49C5D30675B31681AAAB21CF6DDCB2889CE
SHA-512:	8D748EE73E773170B8FE011FE9CE3D9A8DF5A3A15191616382B57EF63217927CFFC0DDCC37274E0D3510A74F507B3A876863426CC1A83854B46582D1E0822178
Malicious:	false
Reputation:	unknown
Preview:	LHEPQ|..K..h_..d<...L.(.K.vc.z]..Z5...B..(..6..b....v.j......g....66.B.3./%U`...zI.....I...c...v...S.....6.G....+.`.H}....v....<.....U.....Jx....].....E....[..{Wg~.KT.....K.%x.....~|..c.F....jd. ...w.....=.+.$,H.....e..ai...pt...G...Z..2.I.O.$.%.]...;08l.ESN..Q.[gu..H...@z....N.`Z...M..s7.}.....4.`;e..\.(.r.M..t.....(U...f.U\.I....1....."p..xv5+...U.*.h0..S..5.U.m.e.f0.n2V&1.-]..M.t.@.kg..b.n;.l@.0K.W>.!BX.,.."...=.dG..Gt....p...h'.'...v[q...H..^>.Y.....Nr.D..$T.....y.d.=.._mN.....4e...S....^....).h"K...Z.....}....<Ap.~....d...2..!...n. .MJ..M..@.e.i.=.. .X...qpw+.J0.C.q...o.n..\..-W.c.$vP;0..EA...J.L.....C.1...E.D7'|:...=P.3.HB..K1..A$./S...,.X....t..t.2..E.w.c..._..Vf.Akd..1\..%.q...gW.h..X'.-...f$x'..KV..!...5tx$.z.e.&.(w.wC.... ..m.!yA.\.Ff.~?..}@B.j.....A...B....-.zX..RL..b...5O9.....Ta....b.[\|k....h..2....K3..k...-&.'..^....:...;F^..!..'XL.ID..Q!$i.[.G.<....."K...x.m.A>..1U..y..R.;F}c.).EU.&.....0.[+.

C:\Users\user\Desktop\LIJDSFKJZG.pdf

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.8671823427657745
Encrypted:	false
SSDEEP:	24:h+y5aezTrmewLFFDwXV7J7y1SOq3HgP+TbhqjcUSxtOQOrS8IC1BMibD:c8aePa/Fxwn0q3HhqOMn2hCBMwD
MD5:	ECEC46F711CC3D43B39194545EB8CAFE
SHA1:	5F1068B5724D6C73D3A47A9C802DDF66FB41CD98
SHA-256:	F5043C47B26A0E1783A136E5D3118A80CD69BC1079ADF3A0D28CEA67A9DB0D5A
SHA-512:	3BBA20211D520E99E863496C35C325C6FA7A750BC5B76C0CD6B27316BF0883D324445C5901C1B7F693FDDD672C727BDED0ED14A3756A5E2A868AEDF698F381 2
Malicious:	false
Reputation:	unknown
Preview:	LIJDS.\\..m.#.....*.....t.g...k.O;..[.*.Zb...}jS..,.....R....M..8.....)4.....@#Pz..%..).q&....{.P.M!.<..Z.f...:....+..a.."..y..|..r..F....=i.n..F..7;..T7C=...b.-...b..J.....x..!...,...1...(....B..._...r ?,bV|.Z#iG....2.L..6..-.f'w?F..a.....`=_....VH..h.j.t...\.Z...*.f..b..'...T ...7=.hr..2..Q ..)rl.+..l72a`...NMy.$....r/Z...2p..d..G?:..7K..'!p....4q..y..U^O}7.0.....u+.f(E..B..n;..w...Xh. h &.\.._.1.#..!z.}.'&Z.t.]x..*.....w....q+..mphO..jB.....l....x....X.....=..&....,.{.....Y&O.b.....d...>.....E..*,..=.U,.....K?..SQ....i..9..V.....G.:g.;.~N..X..oL.X.....9.O...}.KD.".P. v..er. {..>..+<.{...t.r.${=.<.U...^Z...:,i..P....TL...0|..o..Y.+.....5..`jb....q...3l.....X.....K..1....;...|...l.....\_..p0...%..rUva...x..!j.R....`f.\..gx...V.t. |...'xY...;.....nJ....O..r.N.Jl..g.....7v.YK.r ..t..Y;....Em.A...I..-.....x.W.....!.i..R9...!;..a.s.,..0%...a&v..I}.V.F....c...s.I@;F.AJ?.....).@>.sHZ.?././.rR((3.N.....7.[.{#.....\

C:\Users\user\Desktop\LIJDSFKJZG.pdf.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.8671823427657745
Encrypted:	false
SSDEEP:	24:h+y5aezTrmewLFFDwXV7J7y1SOq3HgP+TbhqjcUSxtOQOrS8IC1BMibD:c8aePa/Fxwn0q3HhqOMn2hCBMwD
MD5:	ECEC46F711CC3D43B39194545EB8CAFE

SHA1:	5F1068B5724D6C73D3A47A9C802DDF66FB41CD98
SHA-256:	F5043C47B26A0E1783A136E5D3118A80CD69BC1079ADF3A0D28CEA67A9DB0D5A
SHA-512:	3BBA20211D520E99E863496C35C325C6FA7A750BC5B76C0CD6B27316BF0883D324445C5901C1B7F693FDDD672C727BDED0ED14A3756A5E2A868AEDF698F3812
Malicious:	false
Reputation:	unknown
Preview:	LIJDS.\\..m.#.....*.....t.g...k.O;..[.*.Zb...}jS..,.....R....M..8.....)4.....@#Pz..%..).q&....{.P.M!.<..Z.f...:....+..a.."..y..|..r..F....=i.n..F..7;..T7C=...b.-...b..J.....x..!...,...1...(....B..._...r?,bV|.Z#iG....2.L..6..-.f'w?F..a.....`=_....VH..h.j.t...\.Z...*.f..b..'...T ...7=.hr..2..Q ..)rl.+..l72a`...NMy.$....r/Z...2p..d..G?:..7K..'lp....4q..y..U^O}7.0.....u+.f(E..B..n;..w...Xh. h&.\.._.1.#..!z.}.'&Z.t.]x..*.....w....q+..mphO..jB.....l....x....X.....=..&....,.{.....Y&O.b.........d...>.....E..*,..=.U,.....K?..SQ....i..9..V.....G.:g.;.~N..X..oL.X.....9.O...}.KD.".P. v..er.{..>..+<.{...t.r.${=.<.U...^Z...:,i..P....TL...0|..o..Y.+.....5..`jb....q...3l.....X.....K..1....;...|...l.....,_.p0...%..rUva...x..!j.R....`f.\..gx...V.t. |...'xY...;.....nJ....O..r.N.Jl..g.....7v.YK.r..t..Y;....Em.A...l..-.....x.W.....!.i..R9...!;..a.s.,..0%...a&v..I}.V.F....c...s.I@;F.AJ?.....).@>.sHZ.?././.rR((3.N.....7.[.{#.....\

C:\Users\user\Desktop\NIRMEKAMZH.png

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.861120015473619
Encrypted:	false
SSDEEP:	24:lMzyvNadOQow6jyvAMXiOvto1jPggdilaehquHNTbBY7eWMRIXHUJue8LbD:l9LQ9kyvAMXjy1bggdilTBzRlkAe8vD
MD5:	45DE4B5C5F86045EAA2707CFC80BB2AF
SHA1:	7C32A32BAC17B0E8900AABAE37A6AC032F771963
SHA-256:	D736145CED5866BAE90ECBF713EFCE19C02D59CA26B8D407FFE3623C88F206CE
SHA-512:	C9BC75173739AD97EFA1C2A2D4ACAF15C32E8CBFC037879E009221B77530EE72EFC8079D8C17F1D2A04EB98B0D77A98B157E8F0B893F025D0939226EE40B1FB
Malicious:	false
Reputation:	unknown
Preview:	NIRME.>.....#.D....W....j.s...:.d...T.].....Ll..1...'M(b,.....Ap<H_.E.....W'.5n.T..w..Qn.F../m-9.Z."X:..S..e.'.....cyg.'...-t...=(..5.USaefE.... .D_....!d...?....v....g_.X.z'....E7.?d.Vxp.....{X...~..C.k.t..GjG.U._.j.;(..B..x.....l3S.Lq.y.51.^.....M....I..4...A ..5..l..W.6....NU.'F-`..!.@..@...z4.".c.AK...B.5.<7C.w....%.0l..h.....C.....2.. `Q...K-../r]A~..n....O...)...'.T.bK.....O.o...Y.....l..._..lsB..._.*4+.....|..D...S..p2R.*...*....M|.D..Q...Y<<riw.W..)...^.c.B.e.R..F].v...d.....e2@'.{m...3zxK..h.[.\u.5~.fQ..6`.7...|O.D|..8P.W.n.S.....lJ...A.C(.^...."e.?...l.....)...v.,...d..... !.S.gZ.....A'.N..>..Z...^+.Q....=C.y.w.....Lj}Y8..R..o....|.F..~.f&nOyx}.Dj.m...C.=Q....Oy^j..&dL~....N...b^t...a.....H/.*.f8....5.X.4WN...cl.DZ..>b...J.....i.Gly...l.....h.eqrs.0OQ..K.>.....k...gS"iH.cVy.'...~.w.l./q....oY...f.~.[..BP...;..qg..%n...._j..Fu?..!%y....~.~. $..]i.....YA...J..._...R.k.*../.....)p"&..."..e....UM.v...>.:)D

C:\Users\user\Desktop\NIRMEKAMZH.png.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.861120015473619
Encrypted:	false
SSDEEP:	24:lMzyvNadOQow6jyvAMXiOvto1jPggdilaehquHNTbBY7eWMRIXHUJue8LbD:l9LQ9kyvAMXjy1bggdilTBzRlkAe8vD
MD5:	45DE4B5C5F86045EAA2707CFC80BB2AF
SHA1:	7C32A32BAC17B0E8900AABAE37A6AC032F771963
SHA-256:	D736145CED5866BAE90ECBF713EFCE19C02D59CA26B8D407FFE3623C88F206CE
SHA-512:	C9BC75173739AD97EFA1C2A2D4ACAF15C32E8CBFC037879E009221B77530EE72EFC8079D8C17F1D2A04EB98B0D77A98B157E8F0B893F025D0939226EE40B1FB
Malicious:	false
Reputation:	unknown
Preview:	NIRME.>.....#.D....W....j.s...:.d...T.].....Ll..1...'M(b,.....Ap<H_.E.....W'.5n.T..w..Qn.F../m-9.Z."X:..S..e.'.....cyg.'...-t...=(..5.USaefE.... .D_....!d...?....v....g_.X.z'....E7.?d.Vxp.....{X...~..C.k.t..GjG.U._.j.;(..B..x.....l3S.Lq.y.51.^.....M....I..4...A ..5..l..W.6....NU.'F-`..!.@..@...z4.".c.AK...B.5.<7C.w....%.0l..h.....C.....2.. `Q...K-../r]A~..n....O...)...'.T.bK.....O.o...Y.....l..._..lsB..._.*4+.....|..D...S..p2R.*...*....M|.D..Q...Y<<riw.W..)...^.c.B.e.R..F].v...d.....e2@'.{m...3zxK..h.[.\u.5~.fQ..6`.7...|O.D|..8P.W.n.S.....lJ...A.C(.^...."e.?...l.....)...v.,...d..... !.S.gZ.....A'.N..>..Z...^+.Q....=C.y.w.....Lj}Y8..R..o....|.F..~.f&nOyx}.Dj.m...C.=Q....Oy^j..&dL~....N...b^t...a.....H/.*.f8....5.X.4WN...cl.DZ..>b...J.....i.Gly...l.....h.eqrs.0OQ..K.>.....k...gS"iH.cVy.'...~.w.l./q....oY...f.~.[..BP...;..qg..%n...._j..Fu?..!%y....~.~. $..]i.....YA...J..._...R.k.*../.....)p"&..."..e....UM.v...>.:)D

C:\Users\user\Desktop\NWCXBPIUYI.docx

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.842703177113634
Encrypted:	false
SSDEEP:	24:qQlSqZumfsFFQ5m9ISa1KHn4yTxBipZHdw6PeOZ0+vUwRfj22y3PPNiD+bD:8eya5m9lp1GcZHi6PRZ0CUwEX/Pg4D
MD5:	123F0D7F8FDA4C330F13BCBCDCE293E7

SHA1:	816D9D563924295FEE5C25ACA2892779547A8FB8
SHA-256:	5C004B45D4B5A7ED7C584251CC39D5A1D6ACB353E6CC70455670CF7212F521DA
SHA-512:	168792C40BFA9AEC2E725F42786DEB6D63AA75E0146915225C61ECA033A8A975A721B345C1D7CB6F3E7BDEB1B9DEC99FE1B1037DB39FB0A6E6A0CF8075450AF1
Malicious:	false
Reputation:	unknown
Preview:	NWCXB.8dE.'....@.D>..]Z.W^i....v..T..c..9.DV.....?...*f'c..8SJ?!.....t.r=).hiQ...u.5L]R.8..9.Y6A....$q...nFqF...>..8@{:....nA7dP..r..G...#W.e..sQ.E.+.....k+..\|4.....h.5:V._. .6((.....!M.*..2.PK.<..3..@u..j.....rLGP..x.....#....Ce7.CH.d~..\|U7.....1...%.VP(x...N2...$x9.sh..r[.*...s..QT1.....P....: .fL.....|w..EN.F..X.4Q..C..?.....UX..3.H.#P.2@._...$~.... ...wU..p...-"B....).5...[K.6...~.)..... .gi.^d.?y..0.....K.....K!.#..H.|....>|...3..S.L..f.<..y.....X...2..-r3...".wR8R..:.nDo.....0.h&bn..&...q.N.=..^D.@.?.+.k.....hl.D.F.?.w.,gt .'.Nm..0P.PX.\...r.....S8...._..4....T3.Kkp....J...Au0..a#.2..Y.1~.q.P..|[..l\..U.@...8x...E\..."r..n.b..2....mx.j.q.kt.....9Xi..L.\V*.l.p....Z?E.KH.....1...9..|Z.HHm.....^.=.0.... ..u.7.mP...;"G0.=5.z.#....o.y...l....o...5...%.liU...6Y>.....p:..y...'..kW.....`...e.9>...S..>G.O.....G.tR.!....G.._....n.#..h%.\.~..)d.v..Cn%.....O..5.....I'>\..<...^.Sg.S...V=.*...HAC.i ...Px...._

C:\Users\user\Desktop\NWCXBPIUYI.docx.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.842703177113634
Encrypted:	false
SSDEEP:	24:qQlSqZumfsFFQ5m9ISa1KHn4yTxBipZHdw6PeOZ0+vUwRfj22y3PPNiD+bD:8eya5m9Ip1GcZHi6PRZ0CUwEX/Pg4D
MD5:	123F0D7F8FDA4C330F13BCBCDCE293E7
SHA1:	816D9D563924295FEE5C25ACA2892779547A8FB8
SHA-256:	5C004B45D4B5A7ED7C584251CC39D5A1D6ACB353E6CC70455670CF7212F521DA
SHA-512:	168792C40BFA9AEC2E725F42786DEB6D63AA75E0146915225C61ECA033A8A975A721B345C1D7CB6F3E7BDEB1B9DEC99FE1B1037DB39FB0A6E6A0CF8075450AF1
Malicious:	false
Reputation:	unknown
Preview:	NWCXB.8dE.'....@.D>..]Z.W^i....v..T..c..9.DV.....?...*f'c..8SJ?!.....t.r=).hiQ...u.5L]R.8..9.Y6A....$q...nFqF...>..8@{:....nA7dP..r..G...#W.e..sQ.E.+.....k+..\|4.....h.5:V._. .6((.....!M.*..2.PK.<..3..@u..j.....rLGP..x.....#....Ce7.CH.d~..\|U7.....1...%.VP(x...N2...$x9.sh..r[.*...s..QT1.....P....: .fL.....|w..EN.F..X.4Q..C..?.....UX..3.H.#P.2@._...$~.... ...wU..p...-"B....).5...[K.6...~.)..... .gi.^d.?y..0.....K.....K!.#..H.|....>|...3..S.L..f.<..y.....X...2..-r3...".wR8R..:.nDo.....0.h&bn..&...q.N.=..^D.@.?.+.k.....hl.D.F.?.w.,gt .'.Nm..0P.PX.\...r.....S8...._..4....T3.Kkp....J...Au0..a#.2..Y.1~.q.P..|[..l\..U.@...8x...E\..."r..n.b..2....mx.j.q.kt.....9Xi..L.\V*.l.p....Z?E.KH.....1...9..|Z.HHm.....^.=.0.... ..u.7.mP...;"G0.=5.z.#....o.y...l....o...5...%.liU...6Y>.....p:..y...'..kW.....`...e.9>...S..>G.O.....G.tR.!....G.._....n.#..h%.\.~..)d.v..Cn%.....O..5.....I'>\..<...^.Sg.S...V=.*...HAC.i ...Px...._

C:\Users\user\Desktop\NWCXBPIUYI.jpg

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.854984596398809
Encrypted:	false
SSDEEP:	24:yTxPUzSY0b8l3Tl3xw6GdTlUng4Ddu+9UDPCVLhfc+fgRuK0RiiJbD:yTx18lavGJVvjVeCUZipD
MD5:	825A99CBA581683E404E1970A0A48F86
SHA1:	7D0BAFA8DB1E473A9A90FEA96DB7447E356B8ADE
SHA-256:	EF8BC7DD80C7C3B3F7AC5428CF060D22E0E6227A48F21DFCD60B5ACE5FD3D70A
SHA-512:	D6C5E490835E7766425AB005734A3CE8E1D17565B19D58638F1466D6D9369A91F594BE1283BC05A31B34B185F8884DFCEF2F08898A1D99E21F88B799F5D13B83
Malicious:	**true**
Reputation:	unknown
Preview:	NWCXBp.8.z.....-.d._!.....@..#X.."......Y..U.......cM.x~.s..T.H.........Q$4..9.w~.k.....x..^5...j.%..S.o..]...1..f.M....3...U.F.A.4.?..7..uO..s`.}.@{+...e.....7<..&oY#r...r...z.\.=.G.q..... B...r.....)A.L.V...q.9:..\..X....tC.U.....}....m....%..F..\...X...T*.S..V..2....Z..W.......7.IV...;.....QQ.~..k^.dl.,(@r...`Lg...}.{....x.S..)f.....I.....I..,.....BI.f.....\.....W...?...U!/e...2....v&S.\... .....x....b{.@...d.[..{.....eX.r..A.{...l....#r.....%.t...L.-..._.c.N.`...noT=a..dEg.Q.....\.....y{..c.C.O... 5.u....P.Qg.....\|.H.c....,.h:..w`I...G.0 .[...1L.....a..[.V+.).:,a~..V0dG..N.....!..A. .C]!.....,.h.yG8Y.$..`|.).%..< .?..YP..<..P.J.&gR..#.|..t.....5.}..[^u....D d.].fF....`Pk.}..8:..d3=.<.....H...t.8.P..u....U...)8p....N.6.pk..xV...H.).=..5eg.B...t..t.....9.'.....?+.....e... .y8G..@.R.H..t..I.i.._...3...-I...Y....!..*.c0.9Uf.D._..u..5.x*d..?...SJ.....=..u....W.:|.&.!.7.M..5.....W..hX..J~*.-.O%..}..p".b

C:\Users\user\Desktop\NWCXBPIUYI.jpg.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.854984596398809
Encrypted:	false
SSDEEP:	24:yTxPUzSY0b8l3Tl3xw6GdTlUng4Ddu+9UDPCVLhfc+fgRuK0RiiJbD:yTx18lavGJVvjVeCUZipD
MD5:	825A99CBA581683E404E1970A0A48F86

SHA1:	7D0BAFA8DB1E473A9A90FEA96DB7447E356B8ADE
SHA-256:	EF8BC7DD80C7C3B3F7AC5428CF060D22E0E6227A48F21DFCD60B5ACE5FD3D70A
SHA-512:	D6C5E490835E7766425AB005734A3CE8E1D17565B19D58638F1466D6D9369A91F594BE1283BC05A31B34B185F8884DFCEF2F08898A1D99E21F88B799F5D13B83
Malicious:	false
Reputation:	unknown
Preview:	NWCXBp.8.z.....-.d._!.....@..#X.."......Y..U.......cM.x~.s..T.H.....Q$4..9.w~.k.....x..^5...j.%..S.o..]...1..f.M....3...U.F.A.4.?..7..uO..s`.}.@{+...e.....7<..&oY#r...r...z.\.=.G.q..... B...r.....)A.L.V...q.9:..\..X....tC.U.....}....m....%..F..\...X...T*.S..V..2....Z..W.....7.IV...;.....QQ.~..k^.dl.,(@r...`Lg...}.{....x.S..)f.....I.....I..,.....BI.f.....\.....W...?...U!/e...2....v&S.\... .....x....b{.@...d.[..{.....eX.r..A.{...l....#r.....%.t...L.-..._.c.N.`...noT=a..dEg.Q.....\.....y{..c.C.O... 5.u....P.Qg.....|.H.c....,.h:..w`I...G.0 .[...1L.....a..[.V+.).;.a~..V0dG..N.....I..A. .C]!.....,.h.yG8Y.$..`|.).%..< .?..YP..<..P.J.&gR..#.|..t.....5.}..[^u....D d.].fF....`Pk.}..8:..d3=.<.....H...t.8.P..u....U...)8p....N.6.pk..xV...H.).=..5eg.B...t..t.....9.'.....?+.....e... .y8G..@.R.H..t..l.i.._...3...-I...Y....!..*.c0.9Uf.D._..u..5.x*d..?...SJ.....=..u....W.:|.&.!.7.M..5.....W..hX..J~*.-.O%..}..p".b

C:\Users\user\Desktop\NWCXBPIUYI.xlsx

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.846175115409487
Encrypted:	false
SSDEEP:	24:lJ1s6FO4IhT59YFZJFCvHl9rmSau3px71HUKZ1ewzf2S9HE6ql4kbD:lxUfT59oEPFxVZ11D2S26qtuD
MD5:	52168A390BE9F15F0FDF13FD6DA0F234
SHA1:	F348551065FA5C19A9B1FAC115BF4BE5CC6C581F
SHA-256:	E399FC4C7FEF398449FF76137BBEFE0CD8132384A9B35E3ECE6BB95F1BA46ACC
SHA-512:	9A687ADA5FAA256DE1590290D8EE6DC9FDD3558B7FF7759FD703A6BAFF0D098843C76069A4A08389DB7C4F75B8C84201B47337354E47666CBD798D914621595
Malicious:	false
Reputation:	unknown
Preview:	NWCXB..]..&..:..IM.....f0.,1oi...u.-..o..b.... .F.eQ...m`+2.H...Q.&.....0V.A..-..G....q.6.UsP....j\.2.[...Z....;Z^5..H.....g.9.!.4`.....TE.).0.F..q.>..I..!X.^.-....$::.=>.!.0 ....o..9...T...f.^.5...).7.T...K.J.#[).....M.-e.....c.:....4P.7..j8...!...7oE.]V8....5./.H)m.Y6.....w..I..Z(!.bu..Gh...I.U.....#....L&..m...`B.....p...L.....)..0.w....E$"..F?.,~.....a.....<.....F.."U..=.....E.> .75W.'-5...c...B..[...2.;,..K..gRJKf...<..3...I.z.H.f..2b...|.I.P.(P1.....UZ.GP.1!..kJ...h...t6..q..C&.H...+..)...1n...i....R....N....S.....:.Y.....Fn...@..+.....x.SD.t....s...J..S./0j'.R)6. .N..v...@.....N.....\\G....3.5<.....^p.....!*hms.....4..*..M}F.OT....D.(N .P+xR.v]..?..@!.d.MTK...35@...H~'.G/....N?.w...$...o..4.qF....r...n..%.51..L.nL.x.\.k...Se..]@.N.]C.. sQ..^8!..^M.~s!.I.#%R..H'.I..$....h.;.n\..?XG..p..t...G...(.....#.t`._..R.....P.;...._;M.b..A.p(.I.2.'....H....{I.T ...T.Q.W."=.y.^.....I.....S8..#...8.N

C:\Users\user\Desktop\NWCXBPIUYI.xlsx.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.846175115409487
Encrypted:	false
SSDEEP:	24:lJ1s6FO4IhT59YFZJFCvHl9rmSau3px71HUKZ1ewzf2S9HE6ql4kbD:lxUfT59oEPFxVZ11D2S26qtuD
MD5:	52168A390BE9F15F0FDF13FD6DA0F234
SHA1:	F348551065FA5C19A9B1FAC115BF4BE5CC6C581F
SHA-256:	E399FC4C7FEF398449FF76137BBEFE0CD8132384A9B35E3ECE6BB95F1BA46ACC
SHA-512:	9A687ADA5FAA256DE1590290D8EE6DC9FDD3558B7FF7759FD703A6BAFF0D098843C76069A4A08389DB7C4F75B8C84201B47337354E47666CBD798D914621595
Malicious:	false
Reputation:	unknown
Preview:	NWCXB..]..&..:..IM.....f0.,1oi...u.-..o..b.... .F.eQ...m`+2.H...Q.&.....0V.A..-..G....q.6.UsP....j\.2.[...Z....;Z^5..H.....g.9.!.4`.....TE.).0.F..q.>..I..!X.^.-....$::.=>.!.0 ....o..9...T...f.^.5...).7.T...K.J.#[).....M.-e.....c.:....4P.7..j8...!...7oE.]V8....5./.H)m.Y6.....w..I..Z(!.bu..Gh...I.U.....#....L&..m...`B.....p...L.....)..0.w....E$"..F?.,~.....a.....<.....F.."U..=.....E.> .75W.'-5...c...B..[...2.;,..K..gRJKf...<..3...I.z.H.f..2b...|.I.P.(P1.....UZ.GP.1!..kJ...h...t6..q..C&.H...+..)...1n...i....R....N....S.....:.Y.....Fn...@..+.....x.SD.t....s...J..S./0j'.R)6. .N..v...@.....N.....\\G....3.5<.....^p.....!*hms.....4..*..M}F.OT....D.(N .P+xR.v]..?..@!.d.MTK...35@...H~'.G/....N?.w...$...o..4.qF....r...n..%.51..L.nL.x.\.k...Se..]@.N.]C.. sQ..^8!..^M.~s!.I.#%R..H'.I..$....h.;.n\..?XG..p..t...G...(.....#.t`._..R.....P.;...._;M.b..A.p(.I.2.'....H....{I.T ...T.Q.W."=.y.^.....I.....S8..#...8.N

C:\Users\user\Desktop\NWCXBPIUYI\GNLQNHOLWB.mp3

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.830156468353167
Encrypted:	false
SSDEEP:	24:Zq8/aexzesYprL3xfH6M/x1ZtUL6RKy0Wxwmd8Aw9Qgc+R3b+ma9a9A/Gc9ynb5Z:ZnxDYpfBfH6CDZtu0xwqplE3NCHucUnL
MD5:	B9FB8915A21878EC12E2E6178E37039F
SHA1:	E4431363E4DFC3D46842DCDA0A1CE0838CD7CDD1
SHA-256:	A70EBE43C464C5571B5624D6D80EF71865924301445B813F6DCF82C860AA79DC

SHA-512:	16A58C5AE14863AA01B18606D1699E4D652FA634A6188C8D2B51D14300E5A0AABC4DE9D738CBF509E9197390BD127EEC52893D432152D451871C7333A848A4B
Malicious:	false
Reputation:	unknown
Preview:	GNLQN...(..]v^.dL..P}{..7 ..y.7./..~.L0h.^/v.#.Xu.[.%!^.....A..f1... o.w.....Y..E7..x.ob..!..O...c....PW.s..$.+s./.>z..L..f....`<=..y..>.....9.T..A.j.ilx.;..YJ..v..o.r.^f.=D.. o.....`..j.. c.r[..b{..-.3x..YLg..p.e.l.h:..w...?.!~.w.....FS.....(.U..0...%..x..B.`.e6...*..W...".Cy....F...Z,.z.#..1..P.lr.5...,..*3...Mv...#....^.....Y...0.I.$.....Bc.....0....1.?.fJ6h...%{7c...=.....3eB(W. (.J..<....2G.QfMDY.....mw..}..^.].U.. .T%..LH.5\N3....qYNr2.....G.`...A...L.n.;.....:o...q....[f.W@FA>u0.....a...d.L.I.1..}.f.....2r.-=.4.K@(.TBD.dBA.....$S...N.....L....Nr..I*..]... .*.W.t.'T{.....~.A.....jG...`~7.....w.L.[.{x..a..0.....a..h...0B.7\...Zh.s.Ul^.....Y.....;.``..p..q.:Xf~...t..nQ....."...;G_B.@*m..J....Y...j..U.E#..rX....2$...F.....K.OP.....F.....K.....v wfr.W.C...r..\P.(q...r...C.L..n.~#....3Sb..~....u..a_9..n...>y.CFA..,.|M.....8.oN.6x.Hj..;?y.j.lt.{.sR.v.1..G..7a...F...7....O)...y6....2.....wP...#..q%.3....I}X-...K..*.@4..

C:\Users\user\Desktop\NWCXBPIUYI\GNLQNHOLWB.mp3.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.830156468353167
Encrypted:	false
SSDEEP:	24:Zq8/aexzesYprL3xfH6M/x1ZtUL6RKy0Wxwmd8Aw9Qgc+R3b+ma9a9A/Gc9ynb5Z:ZnxDYpfBfH6CDZtu0xwqplE3NCHucUnL
MD5:	B9FB8915A21878EC12E2E6178E37039F
SHA1:	E4431363E4DFC3D46842DCDA0A1CE0838CD7CDD1
SHA-256:	A70EBE43C464C5571B5624D6D80EF71865924301445B813F6DCF82C860AA79DC
SHA-512:	16A58C5AE14863AA01B18606D1699E4D652FA634A6188C8D2B51D14300E5A0AABC4DE9D738CBF509E9197390BD127EEC52893D432152D451871C7333A848A4B
Malicious:	false
Reputation:	unknown
Preview:	GNLQN...(..]v^.dL..P}{..7 ..y.7./..~.L0h.^/v.#.Xu.[.%!^.....A..f1... o.w.....Y..E7..x.ob..!..O...c....PW.s..$.+s./.>z..L..f....`<=..y..>.....9.T..A.j.ilx.;..YJ..v..o.r.^f.=D.. o.....`..j.. c.r[..b{..-.3x..YLg..p.e.l.h:..w...?.!~.w.....FS.....(.U..0...%..x..B.`.e6...*..W...".Cy....F...Z,.z.#..1..P.lr.5...,..*3...Mv...#....^.....Y...0.I.$.....Bc.....0....1.?.fJ6h...%{7c...=.....3eB(W. (.J..<....2G.QfMDY.....mw..}..^.].U.. .T%..LH.5\N3....qYNr2.....G.`...A...L.n.;.....:o...q....[f.W@FA>u0.....a...d.L.I.1..}.f.....2r.-=.4.K@(.TBD.dBA.....$S...N.....L....Nr..I*..]... .*.W.t.'T{.....~.A.....jG...`~7.....w.L.[.{x..a..0.....a..h...0B.7\...Zh.s.Ul^.....Y.....;.``..p..q.:Xf~...t..nQ....."...;G_B.@*m..J....Y...j..U.E#..rX....2$...F.....K.OP.....F.....K.....v wfr.W.C...r..\P.(q...r...C.L..n.~#....3Sb..~....u..a_9..n...>y.CFA..,.|M.....8.oN.6x.Hj..;?y.j.lt.{.sR.v.1..G..7a...F...7....O)...y6....2.....wP...#..q%.3....I}X-...K..*.@4..

C:\Users\user\Desktop\NWCXBPIUYI\HQJBRDYKDE.jpg

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.853154102635187
Encrypted:	false
SSDEEP:	24:xnXYe/nMwVEw5g9YbY45fk1+lyxpjD02QXedOq7zRGmBehZbD:RXFhja9M5fk1dxJD02wSOyzRBOD
MD5:	9CF13F65E6CEB7AB2CA4DA18B9823A45
SHA1:	22BEF8E81CD11E6ED8EAAE5E109D60BF84A79A29
SHA-256:	C35AC8003A04CC9633C2EA91EC00B58A714654ED1C90E8C741FC62F3AE129367
SHA-512:	632C93D7FCAB56590663E064139582E4DF6EB0F63221B0C3A24F035321E12EFFAB6F1AB3B91EBAACD5BB6C188DF15BBCAAE0F54A7267BDFBD6FF37ADBDE32934
Malicious:	false
Reputation:	unknown
Preview:	HQJBR..%.R..)..u..s_we...~<.rw..Jl.pL.H..."'G.QB...U...s.y.....r1.)+....5..m..R...r..H?.....V../q.-..S....f.@..D.l.....}.N....a....1s....:.Xo.&[..E..5...4.#.R...Y.....la(1Q...6..?4.\"q....F5. /.....'.I...a..p0QM..~..^.x.S?.....YB....z.^J.....T....I..r_i....8.;..0.u|.yO.....O.....d...[H.M.....W![..Bx..]....8..#...vj....b.R.....&q#....c$..c....,.pe....M6j...,....L...R....;. (+.U..o(n...&....?|8.W|.y.y.....>We..D.ie..y...../../...Sj....^.}....Iy.@m. .Q..m....jf|...l....s...D.....T..q.e.t.].....E:a..[.....r..$C...z...{B.Y...KT...h...kN7.7...e..0/.p`.a?....AU.gh....*.n....,.....:?...8PV.....)q.....7.Q\.bo.....`...E.\O<...e.#.....g...Sp...|$B..w...x.\.^.JhI...x.....sx.y`.....X..e..]...xv..=...M;..#.C..Qu.....'.`=%U{.]...;...S.>7.PK.'.....W...*W.....),.....n]R.n%.....Z...^..d.P..9.76|g.;C..nW.i...2.f...~.....uNRP2.`J.s.).Ez.z+....x..i....B.....,L..j.MMzN.....

C:\Users\user\Desktop\NWCXBPIUYI\HQJBRDYKDE.jpg.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.853154102635187
Encrypted:	false
SSDEEP:	24:xnXYe/nMwVEw5g9YbY45fk1+lyxpjD02QXedOq7zRGmBehZbD:RXFhja9M5fk1dxJD02wSOyzRBOD
MD5:	9CF13F65E6CEB7AB2CA4DA18B9823A45
SHA1:	22BEF8E81CD11E6ED8EAAE5E109D60BF84A79A29
SHA-256:	C35AC8003A04CC9633C2EA91EC00B58A714654ED1C90E8C741FC62F3AE129367
SHA-512:	632C93D7FCAB56590663E064139582E4DF6EB0F63221B0C3A24F035321E12EFFAB6F1AB3B91EBAACD5BB6C188DF15BBCAAE0F54A7267BDFBD6FF37ADBDE32934

Malicious:	false
Reputation:	unknown
Preview:	HQJBR..%.R..)..u..s_we...~<.rw..Jl.pL.H..."'G.QB...U...s.y.....r1.)+....5..m..R...r..H?.....V../q.-..S....f.@..D.l.....}.N....a....1s....:.Xo.&[..E..5...4.#.R...Y.....la(1Q...6..?4.\"q....F5. /.....'.I...a..p0QM..~..^.x.S?.....YB....z.^J.....T....l..r_i....8.;..0.u|.yO.....O.....d...[H.M.....W![..Bx..]....8..#...vj....b.R.....&q#....c$..c....,.pe....M6j...,....L...R....;.(+.U..o(n...&....?\|8.W\|.y.y.....>We..D.ie..y...../../...Sj....^.}....Iy.@m. .Q..m....jf\|...!....s...D.....T..q.e.t.]..... E:a..[.....r..$C...z...{B.Y...KT...h...kN7.7...e..0/.p`.a?....AU.gh....*.n....,.....:?...8PV.....)q.....7.Q\.bo....`...E.\O<...e.#.....g...Sp...|$B..w...x.\.^.Jhl...x.....sx.y`.....X..e..]...xv..=...M;..#.C..Qu.....'.`=%U{.]...;...S.>7.PK.'.....W...*W.....),.....n]R.n%.....Z...^..d.P..9.76|g.;C..nW.i...2.f...~.....uNRP2.`J.s.).Ez.z+....x..i....B.....,L..j.MMzN.....

C:\Users\user\Desktop\NWCXBPIUYI\LFOPODGVOH.xlsx

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.8415920865244875
Encrypted:	false
SSDEEP:	24:iANa1v72aDtBcmwj2VB0+5rhwuDjQyeoSTTGKtVxAzHgIPSmm1+KtGmXA500QLLE:Ez+mAy0+5rhzQNoEyH2SAKtFp+D
MD5:	EE5298F528E0AFC74547427578148D46
SHA1:	CD2C62F5526AF2035B419F5F3C95B8DC8BFE06A1
SHA-256:	82A3B2856D207872DB2E978AD1EE1C92108FAE28FFE5FC708E68A77B37356C74
SHA-512:	319FE328B82F31CF5618D4EB5716494FE6330F33E937E7BD36F391B9BC75E6F73329F152503CB38FD79E3CA5D3CD058B78AB22B47155BECBC911814960EEEC4C
Malicious:	false
Reputation:	unknown
Preview:	LFOPO..;....$...v.*y..F.!..[.F4.,..U`.U.[.AA.g\|.....p..;.c.M..w.....Ju...y.4.9..a....'n.9.....0..".'.Mt[...!...O.9.Z...q.&.2v&.&.+o.....B.k`{.*tV..... y.z;..9Z.{{.G...,)P.g7.-Y30..p.....F{*(.j0?.c...<.1..z..e.../A..}.2...."........O.>._2...i....."_(.X.0{_k-l.m;.k.^...2....{.....M..4.IV\|K.Q..}...`...u...q.`..A8u8.uB..~.y@<..I.y..{4...."...X.Q...r.v...d....C.V...A.b..&\|.&...]q..^1.}.....S...+d..BiCw..7..~.....e.-.^....(...@v^iC6..D.0..O..-qr...x*.&.....t..8.....T.Bu}.yD...!R..:..E]...$.)y..b%...p.mV..dj..I..!-....J.... ..}.....VB...$J.F/.O..y..Dyl.....3d.....t..R.W...!1.x.L.G.F.9.....3@&..z(.....zu..j.....o.....e1.-.F..B\|..;g.....R.....vR...s.....?C5.n.-]..!..+...K._...M.\2;X.....L.k.....].BA...:.....b..X...$F.%....5..1..../.....>`.....r..r...7.K. ,....*.J...B;.. .!....u.;..C8.Wj.....E..{e.....I.RY...Z...E..>j$f...t.w..S...\|...9.....zk.....{.N..Y0}(P]rN$..6=)m2.k?..L....D.....2QB..G..+...x..<.....~..R.Hr.w..*.

C:\Users\user\Desktop\NWCXBPIUYI\LFOPODGVOH.xlsx.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.8415920865244875
Encrypted:	false
SSDEEP:	24:iANa1v72aDtBcmwj2VB0+5rhwuDjQyeoSTTGKtVxAzHgIPSmm1+KtGmXA500QLLE:Ez+mAy0+5rhzQNoEyH2SAKtFp+D
MD5:	EE5298F528E0AFC74547427578148D46
SHA1:	CD2C62F5526AF2035B419F5F3C95B8DC8BFE06A1
SHA-256:	82A3B2856D207872DB2E978AD1EE1C92108FAE28FFE5FC708E68A77B37356C74
SHA-512:	319FE328B82F31CF5618D4EB5716494FE6330F33E937E7BD36F391B9BC75E6F73329F152503CB38FD79E3CA5D3CD058B78AB22B47155BECBC911814960EEEC4C
Malicious:	false
Reputation:	unknown
Preview:	LFOPO..;....$...v.*y..F.!..[.F4.,..U`.U.[.AA.g\|.....p..;.c.M..w.....Ju...y.4.9..a....'n.9.....0..".'.Mt[...!...O.9.Z...q.&.2v&.&.+o.....B.k`{.*tV..... y.z;..9Z.{{.G...,)P.g7.-Y30..p.....F{*(.j0?.c...<.1..z..e.../A..}.2...."........O.>._2...i....."_(.X.0{_k-l.m;.k.^...2....{.....M..4.IV\|K.Q..}...`...u...q.`..A8u8.uB..~.y@<..I.y..{4...."...X.Q...r.v...d....C.V...A.b..&\|.&...]q..^1.}.....S...+d..BiCw..7..~.....e.-.^....(...@v^iC6..D.0..O..-qr...x*.&.....t..8.....T.Bu}.yD...!R..:..E]...$.)y..b%...p.mV..dj..I..!-....J.... ..}.....VB...$J.F/.O..y..Dyl.....3d.....t..R.W...!1.x.L.G.F.9.....3@&..z(.....zu..j.....o.....e1.-.F..B\|..;g.....R.....vR...s.....?C5.n.-]..!..+...K._...M.\2;X.....L.k.....].BA...:.....b..X...$F.%....5..1..../.....>`.....r..r...7.K. ,....*.J...B;.. .!....u.;..C8.Wj.....E..{e.....I.RY...Z...E..>j$f...t.w..S...\|...9.....zk.....{.N..Y0}(P]rN$..6=)m2.k?..L....D.....2QB..G..+...x..<.....~..R.Hr.w..*.

C:\Users\user\Desktop\NWCXBPIUYI\NIRMEKAMZH.png

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.854371994441411
Encrypted:	false
SSDEEP:	24:/d1ypAFWQE6SY1zuPr4JFUEDuFNYXh3IE5PeLFD19TKGKXw+4GWtbD:/Ahquj4EEx3IE9sX9PKXwjD
MD5:	59E6F12298E86A5D464973BB57A1B977
SHA1:	D7870AC283858D8F169F8D035D72956873F510CE
SHA-256:	2039D2D15E2959D71988CECA903D523304E8B479E93ADA451742184B217DB4AC
SHA-512:	B97A4C2B74F5AC8C3BCE5C060CD8B05123DED00018A370145DBB20139D9109F1E0EF348A6081636B00774284420E9ED90ACBD2FE8DF5AE7722C4E91ED9D5E5B0

Malicious:	false
Reputation:	unknown
Preview:	NIRMEn....0......./=....;,'W<.&..<=../.H.ge..q.O..UT.{..c....W...4.....s..,F.....Y....e...u.m..$I1V..oM.6.._.t.2.<....H*Q.+..Q.. {Y{K.v.c..;|../JCq..er..*>b..x..0V....\.#.!..bD.'..*.,... .....j./..i.....$)dJ..d.|.WQ..+.lp...Pt3.&.Q..$.7.5..&..=*..l!+....._%.u.....2.q.Q.%n1..i._.t.^....z.}.`. ...r..dxCm.a.(....\{.r..f..|...-..5.....V.T...W\..ys...F..2.^..?1..<.G1C3T46.vY`q..$.. ...2...&.MS....<w.....J.~.O.(H.A ....y... i:..R...-...L.4..$..}.D....mi.....'...t..2.oN O8.sj5.[:D>...8....F.[...)...0'5AE1.!;E:.....}.5.w.&.....&x...Pq..u.b...#g.W,A....);r\|:... g.1..H....N[.v5.%i..9@.h5I.....6.m7....h..x.g..x\...[...xDT.....m).>o.L$..S....s...u....W.gH...o.#$....!..{.O.iG.<.xN...?....Z.y..$d..]r.:y...GC.....g...Q...;.T...D.gT3J.i.{.O..q.r..... ..l._..@...O....a....bhf.zlOs.....k..z.W...=.Z;&H....F.....o.t.....G.c.iSP."...clLNO1..:.U4.....6?....X7@.x%.U8p.....TW..9[a.C.h.....-JO...mOo.EZ....#e..G.p.~&N.....

C:\Users\user\Desktop\NWCXBPIUYI\NIRMEKAMZH.png.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\D804.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.854371994441411
Encrypted:	false
SSDEEP:	24:/d1ypAFWQE6SY1zuPr4JFUEDuFNYXh3IE5PeLFD19TKGKXw+4GWtbD:/Ahquj4EEx3IE9sX9PKXwjD
MD5:	59E6F12298E86A5D464973BB57A1B977
SHA1:	D7870AC283858D8F169F8D035D72956873F510CE
SHA-256:	2039D2D15E2959D71988CECA903D523304E8B479E93ADA451742184B217DB4AC
SHA-512:	B97A4C2B74F5AC8C3BCE5C060CD8B05123DED00018A370145DBB20139D9109F1E0EF348A6081636B00774284420E9ED90ACBD2FE8DF5AE7722C4E91ED9D5E5 B0
Malicious:	false
Reputation:	unknown
Preview:	NIRMEn....0......./=....;,'W<.&..<=../.H.ge..q.O..UT.{..c....W...4.....s..,F.....Y....e...u.m..$I1V..oM.6.._.t.2.<....H*Q.+..Q.. {Y{K.v.c..;|../JCq..er..*>b..x..0V....\.#.!..bD.'..*.,... .....j./..i.....$)dJ..d.|.WQ..+.lp...Pt3.&.Q..$.7.5..&..=*..l!+....._%.u.....2.q.Q.%n1..i._.t.^....z.}.`. ...r..dxCm.a.(....\{.r..f..|...-..5.....V.T...W\..ys...F..2.^..?1..<.G1C3T46.vY`q..$.. ...2...&.MS....<w.....J.~.O.(H.A ....y... i:..R...-...L.4..$..}.D....mi.....'...t..2.oN O8.sj5.[:D>...8....F.[...)...0'5AE1.!;E:.....}.5.w.&.....&x...Pq..u.b...#g.W,A....);r\|:... g.1..H....N[.v5.%i..9@.h5I.....6.m7....h..x.g..x\...[...xDT.....m).>o.L$..S....s...u....W.gH...o.#$....!..{.O.iG.<.xN...?....Z.y..$d..]r.:y...GC.....g...Q...;.T...D.gT3J.i.{.O..q.r..... ..l._..@...O....a....bhf.zlOs.....k..z.W...=.Z;&H....F.....o.t.....G.c.iSP."...clLNO1..:.U4.....6?....X7@.x%.U8p.....TW..9[a.C.h.....-JO...mOo.EZ....#e..G.p.~&N.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.585305891932375
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	01860199.exe
File size:	289280
MD5:	3d8207e1ce6762ff10db118bee3bd99b
SHA1:	82a02d6e00de00074b48ba3cc76424a6efe3e6ab
SHA256:	c38267836dde53953018c962a372e8e74153f97932418b682fc653ecfcb7bece
SHA512:	ca346b7fcd302a5d4afbdceb8d4a50f28d14068d9a72ad9960f647f19810d4936d0514a9ecd3fb2a14b87e7f82c0df33aeeb02bfa64beb394f5eb46fa6810d1a
SSDEEP:	3072:1nsNTcFBW0dKNogILXJ6WPLpjHysySMX3YpCUtn5grTtiFmAevZ:qNTcddpgInDtHMn3frTti9
TLSH:	E7542A1392A13C90F9264B769E1FC6E8B65EF5708F197B69325CBA1F0872172C273B11
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...|.....|.....|...H...EX..k...b.....|...c...|...c...|...c...Richb.....PE..L...e..c.....

File Icon

Icon Hash:	454545454545611d

Static PE Info

General

Entrypoint:	0x404e59
Entrypoint Section:	.text
Digitally signed:	false

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x63859465 [Tue Nov 29 05:11:01 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	2d9ed3462f8a74bfd1231e2e9de56b43

Entrypoint Preview

Instruction
call 00007F54A8CFEB13h
jmp 00007F54A8CFA1ADh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F54A8CFA356h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F54A8CFA380h
test ecx, 00000003h
jne 00007F54A8CFA321h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F54A8CFA31Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F54A8CFA364h
test ah, ah
je 00007F54A8CFA356h
test eax, 00FF0000h
je 00007F54A8CFA345h
test eax, FF000000h

Instruction
je 00007F54A8CFA334h
jmp 00007F54A8CFA2FFh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 004012D8h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
mov dword ptr [ebp-04h], eax
pop esi

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [C++] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x284b8	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x26f000	0x19398	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x289000	0xde4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x3150	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x27f7a	0x28000	False	0.786663818359375	data	7.582759753211569	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x29000	0x245844	0x1e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x26f000	0x19398	0x19400	False	0.3791963180693069	data	4.260273203195652	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x289000	0x332e	0x3400	False	0.22581129807692307	data	2.52425334561387	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x26f730	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x2705d8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x270e80	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x273428	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x2744d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x274988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x275830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x2760d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x276640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x278be8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x279c90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x27a618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x27aae8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x27b990	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x27c238	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x27c900	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x27ce68	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x27f410	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x2804b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x280988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x281830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x2820d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x282640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x284be8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x285c90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x286618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_STRING	0x286d20	0x664	data		
RT_STRING	0x287388	0x59e	data		
RT_STRING	0x287928	0x29a	data		
RT_STRING	0x287bc8	0x248	data		
RT_STRING	0x287e10	0x582	data		
RT_GROUP_ICON	0x286a80	0x68	data		
RT_GROUP_ICON	0x274938	0x4c	data		
RT_GROUP_ICON	0x280920	0x68	data		
RT_GROUP_ICON	0x27aa80	0x68	data		
RT_VERSION	0x286ae8	0x238	data		

Imports

DLL	Import
KERNEL32.dll	GetModuleHandleW, IsBadReadPtr, GetConsoleAliasesLengthA, WaitForMultipleObjectsEx, GetPrivateProfileIntA, FreeConsole, GetVersionExW, WritePrivateProfileStructW, MulDiv, GetModuleFileNameW, CreateActCtxA, WritePrivateProfileStringW, ReplaceFileA, GetStringTypeExA, GetStdHandle, GetLogicalDriveStringsA, OpenMutexW, GetLastError, ReadConsoleOutputCharacterA, GetProcAddress, AttachConsole, SleepEx, VirtualAlloc, _hwrite, LoadLibraryA, InterlockedExchangeAdd, LocalAlloc, GetFileType, CreateFileMappingW, FindFirstVolumeMountPointW, GetNumberFormatW, CreateEventW, GetModuleFileNameA, lstrcmpiW, GetModuleHandleA, CreateMutexA, GetFileAttributesExW, GetConsoleCursorInfo, ScrollConsoleScreenBufferA, GetCurrentThreadId, FindAtomW, EnumResourceLanguagesW, DebugBreak, FindNextVolumeA, AddConsoleAliasW, CancelWaitableTimer, GetCommState, WaitForSingleObject, GetLongPathNameA, GetCommandLineA, GetStartupInfoA, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, HeapFree, WideCharToMultiByte, SetHandleCount, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, Sleep, ExitProcess, WriteFile, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, InterlockedDecrement, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapReAlloc, SetFilePointer, GetConsoleCP, GetConsoleMode, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, InitializeCriticalSectionAndSpinCount, HeapSize, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, FlushFileBuffers, CreateFileA, CloseHandle
USER32.dll	CharLowerBuffA
GDI32.dll	GetCharWidthW, EnumFontsW, GetCharABCWidthsFloatW
ADVAPI32.dll	MapGenericMask

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8.8579905 32045695 05/28/23-10:42:32.589547	UDP	2045695	ET TROJAN DNS Query to SmokeLoader Domain (potunulit .org)	57990	53	192.168.2.3	8.8.8.8
192.168.2.3103.100.211.21849720802839238 05/28/23-10:42:49.105133	TCP	2839238	ETPRO TROJAN Blackmoon CnC Activity	49720	80	192.168.2.3	103.100.211.218
192.168.2.38.8.8.8.8539755 32045695 05/28/23-10:42:39.331614	UDP	2045695	ET TROJAN DNS Query to SmokeLoader Domain (potunulit .org)	53975	53	192.168.2.3	8.8.8.8
211.59.14.90192.168.2.380497142036335 05/28/23-10:42:46.297030	TCP	2036335	ET TROJAN Win32/Filecoder.STOP Variant Public Key Download	80	49714	211.59.14.90	192.168.2.3
192.168.2.3123.140.161.24349713802036333 05/28/23-10:42:45.165749	TCP	2036333	ET TROJAN Win32/Vodkagats Loader Requesting Payload	49713	80	192.168.2.3	123.140.161.243
192.168.2.38.8.8.8.8607675 32045695 05/28/23-10:42:51.638861	UDP	2045695	ET TROJAN DNS Query to SmokeLoader Domain (potunulit .org)	60767	53	192.168.2.3	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8596365 32045695 05/28/23-10:42:45.594129	UDP	2045695	ET TROJAN DNS Query to SmokeLoader Domain (potunulit .org)	59636	53	192.168.2.3	8.8.8.8
175.119.10.231192.168.2.380497112036335 05/28/23-10:42:45.790332	TCP	2036335	ET TROJAN Win32/Filecoder.STOP Variant Public Key Download	80	49711	175.119.10.231	192.168.2.3
192.168.2.3175.119.10.23149721802020826 05/28/23-10:42:51.341437	TCP	2020826	ET TROJAN Potential Dridex.Maldoc Minimal Executable Request	49721	80	192.168.2.3	175.119.10.231
192.168.2.3123.140.161.24349713802020826 05/28/23-10:42:45.165749	TCP	2020826	ET TROJAN Potential Dridex.Maldoc Minimal Executable Request	49713	80	192.168.2.3	123.140.161.243
192.168.2.3211.59.14.9049714802833438 05/28/23-10:42:45.438118	TCP	2833438	ETPRO TROJAN STOP Ransomware CnC Activity	49714	80	192.168.2.3	211.59.14.90
192.168.2.38.8.8.8569245 32045695 05/28/23-10:42:38.041315	UDP	2045695	ET TROJAN DNS Query to SmokeLoader Domain (potunulit .org)	56924	53	192.168.2.3	8.8.8.8
192.168.2.3175.119.10.23149721802036333 05/28/23-10:42:51.341437	TCP	2036333	ET TROJAN Win32/Vodkagats Loader Requesting Payload	49721	80	192.168.2.3	175.119.10.231

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:42:32.626749039 CEST	49698	80	192.168.2.3	188.114.97.7
May 28, 2023 10:42:32.643356085 CEST	80	49698	188.114.97.7	192.168.2.3
May 28, 2023 10:42:32.643559933 CEST	49698	80	192.168.2.3	188.114.97.7
May 28, 2023 10:42:32.643846989 CEST	49698	80	192.168.2.3	188.114.97.7
May 28, 2023 10:42:32.643882036 CEST	49698	80	192.168.2.3	188.114.97.7
May 28, 2023 10:42:32.660356998 CEST	80	49698	188.114.97.7	192.168.2.3
May 28, 2023 10:42:32.660419941 CEST	80	49698	188.114.97.7	192.168.2.3
May 28, 2023 10:42:32.794167995 CEST	80	49698	188.114.97.7	192.168.2.3
May 28, 2023 10:42:32.794229984 CEST	80	49698	188.114.97.7	192.168.2.3
May 28, 2023 10:42:32.794404030 CEST	49698	80	192.168.2.3	188.114.97.7
May 28, 2023 10:42:32.801357985 CEST	49698	80	192.168.2.3	188.114.97.7
May 28, 2023 10:42:32.801403999 CEST	49698	80	192.168.2.3	188.114.97.7
May 28, 2023 10:42:32.817797899 CEST	80	49698	188.114.97.7	192.168.2.3
May 28, 2023 10:42:32.817853928 CEST	80	49698	188.114.97.7	192.168.2.3
May 28, 2023 10:42:32.886226892 CEST	80	49698	188.114.97.7	192.168.2.3
May 28, 2023 10:42:32.886286020 CEST	80	49698	188.114.97.7	192.168.2.3
May 28, 2023 10:42:32.886405945 CEST	49698	80	192.168.2.3	188.114.97.7
May 28, 2023 10:42:33.224350929 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:33.469502926 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:33.469827890 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:33.486999035 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:33.931035042 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.219666004 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.219733953 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.219870090 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:34.465065956 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.465104103 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.465127945 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.465153933 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.465260983 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:34.465419054 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:34.709892988 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.709956884 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.710007906 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.710053921 CEST	80	49699	211.119.84.112	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:42:34.710052967 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:34.710103035 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.710150003 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:34.710150957 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.710200071 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.710207939 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:34.710247993 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.710303068 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:34.954205036 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.954272032 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.954317093 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.954428911 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.954431057 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:34.954477072 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.954534054 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:34.954562902 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.954617977 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.954632998 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:34.954668999 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.954749107 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.954766035 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:34.954796076 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.954840899 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.954853058 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:34.954890013 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.954936028 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.954942942 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:34.954983950 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.955030918 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.955041885 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:34.955079079 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:34.955136061 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:35.199152946 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.199218035 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.199345112 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.199345112 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:35.199393034 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.199459076 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:35.199472904 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.199521065 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.199593067 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:35.199688911 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.199764967 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.199811935 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.199835062 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:35.199867010 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.199919939 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:35.199924946 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.199974060 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.200021029 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:35.200021029 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.200067997 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.200114965 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.200118065 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:35.200182915 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.200239897 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:35.200251102 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.200346947 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.200392962 CEST	80	49699	211.119.84.112	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:42:35.200397968 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:35.200439930 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.200484037 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.200486898 CEST	49699	80	192.168.2.3	211.119.84.112
May 28, 2023 10:42:35.200530052 CEST	80	49699	211.119.84.112	192.168.2.3
May 28, 2023 10:42:35.200575113 CEST	80	49699	211.119.84.112	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 28, 2023 10:42:32.589546919 CEST	192.168.2.3	8.8.8.8	0xc257	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:32.904278994 CEST	192.168.2.3	8.8.8.8	0xf86a	Standard query (0)	colisumy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:38.041315079 CEST	192.168.2.3	8.8.8.8	0xd6e3	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:38.355895042 CEST	192.168.2.3	8.8.8.8	0x3c92	Standard query (0)	speedlab.com.eg	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:38.886869907 CEST	192.168.2.3	8.8.8.8	0xde50	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:39.331614017 CEST	192.168.2.3	8.8.8.8	0x243c	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:43.070905924 CEST	192.168.2.3	8.8.8.8	0xb406	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:43.229671001 CEST	192.168.2.3	8.8.8.8	0x2ed4	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.401875973 CEST	192.168.2.3	8.8.8.8	0x77ce	Standard query (0)	colisumy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.431500912 CEST	192.168.2.3	8.8.8.8	0x8f29	Standard query (0)	zexeq.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.761403084 CEST	192.168.2.3	8.8.8.8	0xe73	Standard query (0)	zexeq.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:45.594129086 CEST	192.168.2.3	8.8.8.8	0x8189	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:45.890947104 CEST	192.168.2.3	8.8.8.8	0xf47c	Standard query (0)	colisumy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:47.954268932 CEST	192.168.2.3	8.8.8.8	0xc85b	Standard query (0)	jp.imgjeoi ghw.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:51.638860941 CEST	192.168.2.3	8.8.8.8	0xe5cb	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:54.714950085 CEST	192.168.2.3	8.8.8.8	0x5de4	Standard query (0)	speedlab.com.eg	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:55.529817104 CEST	192.168.2.3	8.8.8.8	0x7a51	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:55.681421041 CEST	192.168.2.3	8.8.8.8	0x53d3	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:56.441360950 CEST	192.168.2.3	8.8.8.8	0xea1d	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.053306103 CEST	192.168.2.3	8.8.8.8	0x1bec	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.214225054 CEST	192.168.2.3	8.8.8.8	0x510a	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.662609100 CEST	192.168.2.3	8.8.8.8	0xe283	Standard query (0)	colisumy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:59.579483986 CEST	192.168.2.3	8.8.8.8	0x96de	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:00.048898935 CEST	192.168.2.3	8.8.8.8	0xe540	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:00.516808987 CEST	192.168.2.3	8.8.8.8	0x54a7	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:00.802059889 CEST	192.168.2.3	8.8.8.8	0x113f	Standard query (0)	colisumy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:02.195458889 CEST	192.168.2.3	8.8.8.8	0xd66d	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:02.941838980 CEST	192.168.2.3	8.8.8.8	0x92d5	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.434844971 CEST	192.168.2.3	8.8.8.8	0x101b	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 28, 2023 10:43:03.660417080 CEST	192.168.2.3	8.8.8.8	0xe0	Standard query (0)	zexeq.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.803510904 CEST	192.168.2.3	8.8.8.8	0x8f41	Standard query (0)	speedlab.com.eg	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.819369078 CEST	192.168.2.3	8.8.8.8	0xb3c7	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:04.294127941 CEST	192.168.2.3	8.8.8.8	0x1e46	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:04.570935965 CEST	192.168.2.3	8.8.8.8	0x85fb	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:06.353408098 CEST	192.168.2.3	8.8.8.8	0x31d6	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.111479998 CEST	192.168.2.3	8.8.8.8	0x3334	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.327681065 CEST	192.168.2.3	8.8.8.8	0x2d2a	Standard query (0)	colisumy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.336113930 CEST	192.168.2.3	8.8.8.8	0x2e88	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.402429104 CEST	192.168.2.3	8.8.8.8	0xa3e4	Standard query (0)	colisumy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.588644981 CEST	192.168.2.3	8.8.8.8	0x46df	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.848572016 CEST	192.168.2.3	8.8.8.8	0x608b	Standard query (0)	colisumy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.851380110 CEST	192.168.2.3	8.8.8.8	0xda79	Standard query (0)	colisumy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:09.456056118 CEST	192.168.2.3	8.8.8.8	0x8697	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:09.716829062 CEST	192.168.2.3	8.8.8.8	0x3a74	Standard query (0)	colisumy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:10.560178041 CEST	192.168.2.3	8.8.8.8	0x1df7	Standard query (0)	zexeq.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:11.273484945 CEST	192.168.2.3	8.8.8.8	0x7c33	Standard query (0)	zexeq.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.075567961 CEST	192.168.2.3	8.8.8.8	0xac40	Standard query (0)	zexeq.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.679893017 CEST	192.168.2.3	8.8.8.8	0xe9c	Standard query (0)	zexeq.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:14.498408079 CEST	192.168.2.3	8.8.8.8	0xe7f0	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:14.852189064 CEST	192.168.2.3	8.8.8.8	0x9473	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:15.460896015 CEST	192.168.2.3	8.8.8.8	0x6efc	Standard query (0)	speedlab.com.eg	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:15.613418102 CEST	192.168.2.3	8.8.8.8	0xfbca	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:15.983059883 CEST	192.168.2.3	8.8.8.8	0x5091	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:16.217313051 CEST	192.168.2.3	8.8.8.8	0xd095	Standard query (0)	colisumy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:16.640816927 CEST	192.168.2.3	8.8.8.8	0xca04	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:17.003221989 CEST	192.168.2.3	8.8.8.8	0x450d	Standard query (0)	colisumy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:18.466842890 CEST	192.168.2.3	8.8.8.8	0x1f9b	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:18.764915943 CEST	192.168.2.3	8.8.8.8	0x2085	Standard query (0)	colisumy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:19.449069977 CEST	192.168.2.3	8.8.8.8	0x3028	Standard query (0)	adsmanager .facebook.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:19.758980036 CEST	192.168.2.3	8.8.8.8	0x1826	Standard query (0)	zexeq.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.059639931 CEST	192.168.2.3	8.8.8.8	0xad6c	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.712938070 CEST	192.168.2.3	8.8.8.8	0xa0b6	Standard query (0)	zexeq.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.815661907 CEST	192.168.2.3	8.8.8.8	0x9518	Standard query (0)	www.facebo ok.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:21.989151955 CEST	192.168.2.3	8.8.8.8	0xe689	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 28, 2023 10:43:22.024241924 CEST	192.168.2.3	8.8.8.8	0x3f8a	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.393553972 CEST	192.168.2.3	8.8.8.8	0xa2d	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.731909990 CEST	192.168.2.3	8.8.8.8	0xe43	Standard query (0)	ss.apjeoighw.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:23.587229967 CEST	192.168.2.3	8.8.8.8	0x5e33	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:23.942609072 CEST	192.168.2.3	8.8.8.8	0x4fc2	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:24.187830925 CEST	192.168.2.3	8.8.8.8	0x30c4	Standard query (0)	colisumy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:25.135301113 CEST	192.168.2.3	8.8.8.8	0x5cc3	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:26.377245903 CEST	192.168.2.3	8.8.8.8	0x36ac	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:28.015558004 CEST	192.168.2.3	8.8.8.8	0xbebf	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:29.523540020 CEST	192.168.2.3	8.8.8.8	0xf4f1	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:30.456631899 CEST	192.168.2.3	8.8.8.8	0x7f	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:30.880661011 CEST	192.168.2.3	8.8.8.8	0x89c9	Standard query (0)	zexeq.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:31.084322929 CEST	192.168.2.3	8.8.8.8	0xc813	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:31.538268089 CEST	192.168.2.3	8.8.8.8	0xea73	Standard query (0)	adsmanager.facebook.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:32.162396908 CEST	192.168.2.3	8.8.8.8	0x72a9	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:32.421588898 CEST	192.168.2.3	8.8.8.8	0x5905	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:33.629355907 CEST	192.168.2.3	8.8.8.8	0x4431	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:34.475882053 CEST	192.168.2.3	8.8.8.8	0x75e7	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:35.990720034 CEST	192.168.2.3	8.8.8.8	0x64e9	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:37.213870049 CEST	192.168.2.3	8.8.8.8	0x6cdd	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:37.239511967 CEST	192.168.2.3	8.8.8.8	0x5481	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:38.759414911 CEST	192.168.2.3	8.8.8.8	0xa202	Standard query (0)	shsplatform.co.uk	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:39.408296108 CEST	192.168.2.3	8.8.8.8	0xa76c	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:40.758038044 CEST	192.168.2.3	8.8.8.8	0xcb14	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:42.292027950 CEST	192.168.2.3	8.8.8.8	0xed1c	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:42.686049938 CEST	192.168.2.3	8.8.8.8	0xd5a1	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:44.206152916 CEST	192.168.2.3	8.8.8.8	0xba0a	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:45.733243942 CEST	192.168.2.3	8.8.8.8	0x8d9d	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:46.970834017 CEST	192.168.2.3	8.8.8.8	0xef30	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:47.335722923 CEST	192.168.2.3	8.8.8.8	0xb441	Standard query (0)	adsmanager.facebook.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:47.361634970 CEST	192.168.2.3	8.8.8.8	0x6476	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:47.854331970 CEST	192.168.2.3	8.8.8.8	0xaa8d	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:48.617662907 CEST	192.168.2.3	8.8.8.8	0xfe12	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:50.046684027 CEST	192.168.2.3	8.8.8.8	0x6bb1	Standard query (0)	ss.apjeoighw.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:50.121634960 CEST	192.168.2.3	8.8.8.8	0x2973	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 28, 2023 10:43:51.641613007 CEST	192.168.2.3	8.8.8.8	0x2561	Standard query (0)	toobussy.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:52.415997028 CEST	192.168.2.3	8.8.8.8	0xcfb6	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:57.150626898 CEST	192.168.2.3	8.8.8.8	0xb748	Standard query (0)	adsmanager.facebook.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:57.771193981 CEST	192.168.2.3	8.8.8.8	0x9b9b	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:59.824630022 CEST	192.168.2.3	8.8.8.8	0xdec8	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false
May 28, 2023 10:44:04.964651108 CEST	192.168.2.3	8.8.8.8	0x92cb	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:42:32.616553068 CEST	8.8.8.8	192.168.2.3	0xc257	No error (0)	potunulit.org		188.114.97.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:32.616553068 CEST	8.8.8.8	192.168.2.3	0xc257	No error (0)	potunulit.org		188.114.96.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:33.222845078 CEST	8.8.8.8	192.168.2.3	0xf86a	No error (0)	colisumy.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:33.222845078 CEST	8.8.8.8	192.168.2.3	0xf86a	No error (0)	colisumy.com		211.171.233.129	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:33.222845078 CEST	8.8.8.8	192.168.2.3	0xf86a	No error (0)	colisumy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:33.222845078 CEST	8.8.8.8	192.168.2.3	0xf86a	No error (0)	colisumy.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:33.222845078 CEST	8.8.8.8	192.168.2.3	0xf86a	No error (0)	colisumy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:33.222845078 CEST	8.8.8.8	192.168.2.3	0xf86a	No error (0)	colisumy.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:33.222845078 CEST	8.8.8.8	192.168.2.3	0xf86a	No error (0)	colisumy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:33.222845078 CEST	8.8.8.8	192.168.2.3	0xf86a	No error (0)	colisumy.com		187.245.185.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:33.222845078 CEST	8.8.8.8	192.168.2.3	0xf86a	No error (0)	colisumy.com		211.119.84.111	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:33.222845078 CEST	8.8.8.8	192.168.2.3	0xf86a	No error (0)	colisumy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:38.075985909 CEST	8.8.8.8	192.168.2.3	0xd6e3	No error (0)	potunulit.org		188.114.97.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:38.075985909 CEST	8.8.8.8	192.168.2.3	0xd6e3	No error (0)	potunulit.org		188.114.96.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:38.384840012 CEST	8.8.8.8	192.168.2.3	0x3c92	No error (0)	speedlab.com.eg		217.174.148.28	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:38.921091080 CEST	8.8.8.8	192.168.2.3	0xde50	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:39.366380930 CEST	8.8.8.8	192.168.2.3	0x243c	No error (0)	potunulit.org		188.114.96.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:39.366380930 CEST	8.8.8.8	192.168.2.3	0x243c	No error (0)	potunulit.org		188.114.97.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:43.096632004 CEST	8.8.8.8	192.168.2.3	0xb406	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:42:43.264162064 CEST	8.8.8.8	192.168.2.3	0x2ed4	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.728355885 CEST	8.8.8.8	192.168.2.3	0x8f29	No error (0)	zexeq.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.728355885 CEST	8.8.8.8	192.168.2.3	0x8f29	No error (0)	zexeq.com		2.180.10.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.728355885 CEST	8.8.8.8	192.168.2.3	0x8f29	No error (0)	zexeq.com		5.163.228.78	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.728355885 CEST	8.8.8.8	192.168.2.3	0x8f29	No error (0)	zexeq.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.728355885 CEST	8.8.8.8	192.168.2.3	0x8f29	No error (0)	zexeq.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.728355885 CEST	8.8.8.8	192.168.2.3	0x8f29	No error (0)	zexeq.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.728355885 CEST	8.8.8.8	192.168.2.3	0x8f29	No error (0)	zexeq.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.728355885 CEST	8.8.8.8	192.168.2.3	0x8f29	No error (0)	zexeq.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.728355885 CEST	8.8.8.8	192.168.2.3	0x8f29	No error (0)	zexeq.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.728355885 CEST	8.8.8.8	192.168.2.3	0x8f29	No error (0)	zexeq.com		211.59.14.90	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.919411898 CEST	8.8.8.8	192.168.2.3	0x77ce	No error (0)	colisumy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.919411898 CEST	8.8.8.8	192.168.2.3	0x77ce	No error (0)	colisumy.com		187.245.185.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.919411898 CEST	8.8.8.8	192.168.2.3	0x77ce	No error (0)	colisumy.com		211.119.84.111	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.919411898 CEST	8.8.8.8	192.168.2.3	0x77ce	No error (0)	colisumy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.919411898 CEST	8.8.8.8	192.168.2.3	0x77ce	No error (0)	colisumy.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.919411898 CEST	8.8.8.8	192.168.2.3	0x77ce	No error (0)	colisumy.com		211.171.233.129	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.919411898 CEST	8.8.8.8	192.168.2.3	0x77ce	No error (0)	colisumy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.919411898 CEST	8.8.8.8	192.168.2.3	0x77ce	No error (0)	colisumy.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.919411898 CEST	8.8.8.8	192.168.2.3	0x77ce	No error (0)	colisumy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:44.919411898 CEST	8.8.8.8	192.168.2.3	0x77ce	No error (0)	colisumy.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:45.156594038 CEST	8.8.8.8	192.168.2.3	0xe73	No error (0)	zexeq.com		211.59.14.90	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:45.156594038 CEST	8.8.8.8	192.168.2.3	0xe73	No error (0)	zexeq.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:45.156594038 CEST	8.8.8.8	192.168.2.3	0xe73	No error (0)	zexeq.com		2.180.10.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:45.156594038 CEST	8.8.8.8	192.168.2.3	0xe73	No error (0)	zexeq.com		5.163.228.78	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:42:45.156594038 CEST	8.8.8.8	192.168.2.3	0xe73	No error (0)	zexeq.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:45.156594038 CEST	8.8.8.8	192.168.2.3	0xe73	No error (0)	zexeq.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:45.156594038 CEST	8.8.8.8	192.168.2.3	0xe73	No error (0)	zexeq.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:45.156594038 CEST	8.8.8.8	192.168.2.3	0xe73	No error (0)	zexeq.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:45.156594038 CEST	8.8.8.8	192.168.2.3	0xe73	No error (0)	zexeq.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:45.156594038 CEST	8.8.8.8	192.168.2.3	0xe73	No error (0)	zexeq.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:45.629652977 CEST	8.8.8.8	192.168.2.3	0x8189	No error (0)	potunulit.org		188.114.97.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:45.629652977 CEST	8.8.8.8	192.168.2.3	0x8189	No error (0)	potunulit.org		188.114.96.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:46.216006994 CEST	8.8.8.8	192.168.2.3	0xf47c	No error (0)	colisumy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:46.216006994 CEST	8.8.8.8	192.168.2.3	0xf47c	No error (0)	colisumy.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:46.216006994 CEST	8.8.8.8	192.168.2.3	0xf47c	No error (0)	colisumy.com		211.171.233.129	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:46.216006994 CEST	8.8.8.8	192.168.2.3	0xf47c	No error (0)	colisumy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:46.216006994 CEST	8.8.8.8	192.168.2.3	0xf47c	No error (0)	colisumy.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:46.216006994 CEST	8.8.8.8	192.168.2.3	0xf47c	No error (0)	colisumy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:46.216006994 CEST	8.8.8.8	192.168.2.3	0xf47c	No error (0)	colisumy.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:46.216006994 CEST	8.8.8.8	192.168.2.3	0xf47c	No error (0)	colisumy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:46.216006994 CEST	8.8.8.8	192.168.2.3	0xf47c	No error (0)	colisumy.com		187.245.185.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:46.216006994 CEST	8.8.8.8	192.168.2.3	0xf47c	No error (0)	colisumy.com		211.119.84.111	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:48.303133965 CEST	8.8.8.8	192.168.2.3	0xc85b	No error (0)	jp.imgjeoighw.com		103.100.211.218	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:51.658840895 CEST	8.8.8.8	192.168.2.3	0xe5cb	No error (0)	potunulit.org		188.114.97.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:51.658840895 CEST	8.8.8.8	192.168.2.3	0xe5cb	No error (0)	potunulit.org		188.114.96.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:54.770947933 CEST	8.8.8.8	192.168.2.3	0x5de4	No error (0)	speedlab.com.eg		217.174.148.28	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:55.556116104 CEST	8.8.8.8	192.168.2.3	0x7a51	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:55.709743023 CEST	8.8.8.8	192.168.2.3	0x53d3	No error (0)	potunulit.org		188.114.96.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:55.709743023 CEST	8.8.8.8	192.168.2.3	0x53d3	No error (0)	potunulit.org		188.114.97.7	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:42:56.460953951 CEST	8.8.8.8	192.168.2.3	0xea1d	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.082051992 CEST	8.8.8.8	192.168.2.3	0x1bec	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.233885050 CEST	8.8.8.8	192.168.2.3	0x510a	No error (0)	potunulit.org		188.114.96.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.233885050 CEST	8.8.8.8	192.168.2.3	0x510a	No error (0)	potunulit.org		188.114.97.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.691430092 CEST	8.8.8.8	192.168.2.3	0xe283	No error (0)	colisumy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.691430092 CEST	8.8.8.8	192.168.2.3	0xe283	No error (0)	colisumy.com		187.245.185.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.691430092 CEST	8.8.8.8	192.168.2.3	0xe283	No error (0)	colisumy.com		211.119.84.111	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.691430092 CEST	8.8.8.8	192.168.2.3	0xe283	No error (0)	colisumy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.691430092 CEST	8.8.8.8	192.168.2.3	0xe283	No error (0)	colisumy.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.691430092 CEST	8.8.8.8	192.168.2.3	0xe283	No error (0)	colisumy.com		211.171.233.129	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.691430092 CEST	8.8.8.8	192.168.2.3	0xe283	No error (0)	colisumy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.691430092 CEST	8.8.8.8	192.168.2.3	0xe283	No error (0)	colisumy.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.691430092 CEST	8.8.8.8	192.168.2.3	0xe283	No error (0)	colisumy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:58.691430092 CEST	8.8.8.8	192.168.2.3	0xe283	No error (0)	colisumy.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:42:59.602802038 CEST	8.8.8.8	192.168.2.3	0x96de	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:00.069217920 CEST	8.8.8.8	192.168.2.3	0xe540	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:00.545985937 CEST	8.8.8.8	192.168.2.3	0x54a7	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:01.159085035 CEST	8.8.8.8	192.168.2.3	0x113f	No error (0)	colisumy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:01.159085035 CEST	8.8.8.8	192.168.2.3	0x113f	No error (0)	colisumy.com		187.245.185.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:01.159085035 CEST	8.8.8.8	192.168.2.3	0x113f	No error (0)	colisumy.com		211.119.84.111	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:01.159085035 CEST	8.8.8.8	192.168.2.3	0x113f	No error (0)	colisumy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:01.159085035 CEST	8.8.8.8	192.168.2.3	0x113f	No error (0)	colisumy.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:01.159085035 CEST	8.8.8.8	192.168.2.3	0x113f	No error (0)	colisumy.com		211.171.233.129	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:01.159085035 CEST	8.8.8.8	192.168.2.3	0x113f	No error (0)	colisumy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:01.159085035 CEST	8.8.8.8	192.168.2.3	0x113f	No error (0)	colisumy.com		201.124.33.177	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:01.159085035 CEST	8.8.8.8	192.168.2.3	0x113f	No error (0)	colisumy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:01.159085035 CEST	8.8.8.8	192.168.2.3	0x113f	No error (0)	colisumy.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:02.224514008 CEST	8.8.8.8	192.168.2.3	0xd66d	No error (0)	potunulit.org		188.114.97.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:02.224514008 CEST	8.8.8.8	192.168.2.3	0xd66d	No error (0)	potunulit.org		188.114.96.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:02.961893082 CEST	8.8.8.8	192.168.2.3	0x92d5	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.462907076 CEST	8.8.8.8	192.168.2.3	0x101b	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.689167976 CEST	8.8.8.8	192.168.2.3	0xe0	No error (0)	zexeq.com		211.59.14.90	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.689167976 CEST	8.8.8.8	192.168.2.3	0xe0	No error (0)	zexeq.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.689167976 CEST	8.8.8.8	192.168.2.3	0xe0	No error (0)	zexeq.com		2.180.10.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.689167976 CEST	8.8.8.8	192.168.2.3	0xe0	No error (0)	zexeq.com		5.163.228.78	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.689167976 CEST	8.8.8.8	192.168.2.3	0xe0	No error (0)	zexeq.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.689167976 CEST	8.8.8.8	192.168.2.3	0xe0	No error (0)	zexeq.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.689167976 CEST	8.8.8.8	192.168.2.3	0xe0	No error (0)	zexeq.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.689167976 CEST	8.8.8.8	192.168.2.3	0xe0	No error (0)	zexeq.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.689167976 CEST	8.8.8.8	192.168.2.3	0xe0	No error (0)	zexeq.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.689167976 CEST	8.8.8.8	192.168.2.3	0xe0	No error (0)	zexeq.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.832632065 CEST	8.8.8.8	192.168.2.3	0x8f41	No error (0)	speedlab.com.eg		217.174.148.28	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:03.839757919 CEST	8.8.8.8	192.168.2.3	0xb3c7	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:04.308897972 CEST	8.8.8.8	192.168.2.3	0x1e46	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:04.599715948 CEST	8.8.8.8	192.168.2.3	0x85fb	No error (0)	potunulit.org		188.114.97.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:04.599715948 CEST	8.8.8.8	192.168.2.3	0x85fb	No error (0)	potunulit.org		188.114.96.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:06.382241964 CEST	8.8.8.8	192.168.2.3	0x31d6	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.126195908 CEST	8.8.8.8	192.168.2.3	0x3334	No error (0)	potunulit.org		188.114.97.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.126195908 CEST	8.8.8.8	192.168.2.3	0x3334	No error (0)	potunulit.org		188.114.96.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.356868029 CEST	8.8.8.8	192.168.2.3	0x2d2a	No error (0)	colisumy.com		123.140.161.243	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:08.356868029 CEST	8.8.8.8	192.168.2.3	0x2d2a	No error (0)	colisumy.com		187.245.185.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.356868029 CEST	8.8.8.8	192.168.2.3	0x2d2a	No error (0)	colisumy.com		211.119.84.111	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.356868029 CEST	8.8.8.8	192.168.2.3	0x2d2a	No error (0)	colisumy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.356868029 CEST	8.8.8.8	192.168.2.3	0x2d2a	No error (0)	colisumy.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.356868029 CEST	8.8.8.8	192.168.2.3	0x2d2a	No error (0)	colisumy.com		211.171.233.129	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.356868029 CEST	8.8.8.8	192.168.2.3	0x2d2a	No error (0)	colisumy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.356868029 CEST	8.8.8.8	192.168.2.3	0x2d2a	No error (0)	colisumy.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.356868029 CEST	8.8.8.8	192.168.2.3	0x2d2a	No error (0)	colisumy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.356868029 CEST	8.8.8.8	192.168.2.3	0x2d2a	No error (0)	colisumy.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.364994049 CEST	8.8.8.8	192.168.2.3	0x2e88	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.617041111 CEST	8.8.8.8	192.168.2.3	0x46df	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.797144890 CEST	8.8.8.8	192.168.2.3	0xa3e4	No error (0)	colisumy.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.797144890 CEST	8.8.8.8	192.168.2.3	0xa3e4	No error (0)	colisumy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.797144890 CEST	8.8.8.8	192.168.2.3	0xa3e4	No error (0)	colisumy.com		187.245.185.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.797144890 CEST	8.8.8.8	192.168.2.3	0xa3e4	No error (0)	colisumy.com		211.119.84.111	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.797144890 CEST	8.8.8.8	192.168.2.3	0xa3e4	No error (0)	colisumy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.797144890 CEST	8.8.8.8	192.168.2.3	0xa3e4	No error (0)	colisumy.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.797144890 CEST	8.8.8.8	192.168.2.3	0xa3e4	No error (0)	colisumy.com		211.171.233.129	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.797144890 CEST	8.8.8.8	192.168.2.3	0xa3e4	No error (0)	colisumy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.797144890 CEST	8.8.8.8	192.168.2.3	0xa3e4	No error (0)	colisumy.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.797144890 CEST	8.8.8.8	192.168.2.3	0xa3e4	No error (0)	colisumy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.876914978 CEST	8.8.8.8	192.168.2.3	0x608b	No error (0)	colisumy.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.876914978 CEST	8.8.8.8	192.168.2.3	0x608b	No error (0)	colisumy.com		211.171.233.129	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.876914978 CEST	8.8.8.8	192.168.2.3	0x608b	No error (0)	colisumy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.876914978 CEST	8.8.8.8	192.168.2.3	0x608b	No error (0)	colisumy.com		201.124.33.177	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:08.876914978 CEST	8.8.8.8	192.168.2.3	0x608b	No error (0)	colisumy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.876914978 CEST	8.8.8.8	192.168.2.3	0x608b	No error (0)	colisumy.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.876914978 CEST	8.8.8.8	192.168.2.3	0x608b	No error (0)	colisumy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.876914978 CEST	8.8.8.8	192.168.2.3	0x608b	No error (0)	colisumy.com		187.245.185.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.876914978 CEST	8.8.8.8	192.168.2.3	0x608b	No error (0)	colisumy.com		211.119.84.111	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.876914978 CEST	8.8.8.8	192.168.2.3	0x608b	No error (0)	colisumy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.879879951 CEST	8.8.8.8	192.168.2.3	0xda79	No error (0)	colisumy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.879879951 CEST	8.8.8.8	192.168.2.3	0xda79	No error (0)	colisumy.com		187.245.185.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.879879951 CEST	8.8.8.8	192.168.2.3	0xda79	No error (0)	colisumy.com		211.119.84.111	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.879879951 CEST	8.8.8.8	192.168.2.3	0xda79	No error (0)	colisumy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.879879951 CEST	8.8.8.8	192.168.2.3	0xda79	No error (0)	colisumy.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.879879951 CEST	8.8.8.8	192.168.2.3	0xda79	No error (0)	colisumy.com		211.171.233.129	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.879879951 CEST	8.8.8.8	192.168.2.3	0xda79	No error (0)	colisumy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.879879951 CEST	8.8.8.8	192.168.2.3	0xda79	No error (0)	colisumy.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.879879951 CEST	8.8.8.8	192.168.2.3	0xda79	No error (0)	colisumy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:08.879879951 CEST	8.8.8.8	192.168.2.3	0xda79	No error (0)	colisumy.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:09.484451056 CEST	8.8.8.8	192.168.2.3	0x8697	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:09.736618042 CEST	8.8.8.8	192.168.2.3	0x3a74	No error (0)	colisumy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:09.736618042 CEST	8.8.8.8	192.168.2.3	0x3a74	No error (0)	colisumy.com		187.245.185.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:09.736618042 CEST	8.8.8.8	192.168.2.3	0x3a74	No error (0)	colisumy.com		211.119.84.111	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:09.736618042 CEST	8.8.8.8	192.168.2.3	0x3a74	No error (0)	colisumy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:09.736618042 CEST	8.8.8.8	192.168.2.3	0x3a74	No error (0)	colisumy.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:09.736618042 CEST	8.8.8.8	192.168.2.3	0x3a74	No error (0)	colisumy.com		211.171.233.129	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:09.736618042 CEST	8.8.8.8	192.168.2.3	0x3a74	No error (0)	colisumy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:09.736618042 CEST	8.8.8.8	192.168.2.3	0x3a74	No error (0)	colisumy.com		201.124.33.177	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:09.736618042 CEST	8.8.8.8	192.168.2.3	0x3a74	No error (0)	colisumy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:09.736618042 CEST	8.8.8.8	192.168.2.3	0x3a74	No error (0)	colisumy.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:10.580411911 CEST	8.8.8.8	192.168.2.3	0x1df7	No error (0)	zexeq.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:10.580411911 CEST	8.8.8.8	192.168.2.3	0x1df7	No error (0)	zexeq.com		2.180.10.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:10.580411911 CEST	8.8.8.8	192.168.2.3	0x1df7	No error (0)	zexeq.com		5.163.228.78	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:10.580411911 CEST	8.8.8.8	192.168.2.3	0x1df7	No error (0)	zexeq.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:10.580411911 CEST	8.8.8.8	192.168.2.3	0x1df7	No error (0)	zexeq.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:10.580411911 CEST	8.8.8.8	192.168.2.3	0x1df7	No error (0)	zexeq.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:10.580411911 CEST	8.8.8.8	192.168.2.3	0x1df7	No error (0)	zexeq.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:10.580411911 CEST	8.8.8.8	192.168.2.3	0x1df7	No error (0)	zexeq.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:10.580411911 CEST	8.8.8.8	192.168.2.3	0x1df7	No error (0)	zexeq.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:10.580411911 CEST	8.8.8.8	192.168.2.3	0x1df7	No error (0)	zexeq.com		211.59.14.90	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:11.301954031 CEST	8.8.8.8	192.168.2.3	0x7c33	No error (0)	zexeq.com		211.59.14.90	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:11.301954031 CEST	8.8.8.8	192.168.2.3	0x7c33	No error (0)	zexeq.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:11.301954031 CEST	8.8.8.8	192.168.2.3	0x7c33	No error (0)	zexeq.com		2.180.10.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:11.301954031 CEST	8.8.8.8	192.168.2.3	0x7c33	No error (0)	zexeq.com		5.163.228.78	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:11.301954031 CEST	8.8.8.8	192.168.2.3	0x7c33	No error (0)	zexeq.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:11.301954031 CEST	8.8.8.8	192.168.2.3	0x7c33	No error (0)	zexeq.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:11.301954031 CEST	8.8.8.8	192.168.2.3	0x7c33	No error (0)	zexeq.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:11.301954031 CEST	8.8.8.8	192.168.2.3	0x7c33	No error (0)	zexeq.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:11.301954031 CEST	8.8.8.8	192.168.2.3	0x7c33	No error (0)	zexeq.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:11.301954031 CEST	8.8.8.8	192.168.2.3	0x7c33	No error (0)	zexeq.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.095798016 CEST	8.8.8.8	192.168.2.3	0xac40	No error (0)	zexeq.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.095798016 CEST	8.8.8.8	192.168.2.3	0xac40	No error (0)	zexeq.com		2.180.10.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.095798016 CEST	8.8.8.8	192.168.2.3	0xac40	No error (0)	zexeq.com		5.163.228.78	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:12.095798016 CEST	8.8.8.8	192.168.2.3	0xac40	No error (0)	zexeq.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.095798016 CEST	8.8.8.8	192.168.2.3	0xac40	No error (0)	zexeq.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.095798016 CEST	8.8.8.8	192.168.2.3	0xac40	No error (0)	zexeq.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.095798016 CEST	8.8.8.8	192.168.2.3	0xac40	No error (0)	zexeq.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.095798016 CEST	8.8.8.8	192.168.2.3	0xac40	No error (0)	zexeq.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.095798016 CEST	8.8.8.8	192.168.2.3	0xac40	No error (0)	zexeq.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.095798016 CEST	8.8.8.8	192.168.2.3	0xac40	No error (0)	zexeq.com		211.59.14.90	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.700383902 CEST	8.8.8.8	192.168.2.3	0xe9c	No error (0)	zexeq.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.700383902 CEST	8.8.8.8	192.168.2.3	0xe9c	No error (0)	zexeq.com		2.180.10.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.700383902 CEST	8.8.8.8	192.168.2.3	0xe9c	No error (0)	zexeq.com		5.163.228.78	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.700383902 CEST	8.8.8.8	192.168.2.3	0xe9c	No error (0)	zexeq.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.700383902 CEST	8.8.8.8	192.168.2.3	0xe9c	No error (0)	zexeq.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.700383902 CEST	8.8.8.8	192.168.2.3	0xe9c	No error (0)	zexeq.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.700383902 CEST	8.8.8.8	192.168.2.3	0xe9c	No error (0)	zexeq.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.700383902 CEST	8.8.8.8	192.168.2.3	0xe9c	No error (0)	zexeq.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.700383902 CEST	8.8.8.8	192.168.2.3	0xe9c	No error (0)	zexeq.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:12.700383902 CEST	8.8.8.8	192.168.2.3	0xe9c	No error (0)	zexeq.com		211.59.14.90	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:14.518148899 CEST	8.8.8.8	192.168.2.3	0xe7f0	No error (0)	potunulit.org		188.114.97.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:14.518148899 CEST	8.8.8.8	192.168.2.3	0xe7f0	No error (0)	potunulit.org		188.114.96.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:14.872251987 CEST	8.8.8.8	192.168.2.3	0x9473	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:15.519408941 CEST	8.8.8.8	192.168.2.3	0x6efc	No error (0)	speedlab.com.eg		217.174.148.28	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:15.636708021 CEST	8.8.8.8	192.168.2.3	0xfbca	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:16.004530907 CEST	8.8.8.8	192.168.2.3	0x5091	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:16.510293007 CEST	8.8.8.8	192.168.2.3	0xd095	No error (0)	colisumy.com		211.171.233.129	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:16.510293007 CEST	8.8.8.8	192.168.2.3	0xd095	No error (0)	colisumy.com		37.34.248.24	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:16.510293007 CEST	8.8.8.8	192.168.2.3	0xd095	No error (0)	colisumy.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:16.510293007 CEST	8.8.8.8	192.168.2.3	0xd095	No error (0)	colisumy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:16.510293007 CEST	8.8.8.8	192.168.2.3	0xd095	No error (0)	colisumy.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:16.510293007 CEST	8.8.8.8	192.168.2.3	0xd095	No error (0)	colisumy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:16.510293007 CEST	8.8.8.8	192.168.2.3	0xd095	No error (0)	colisumy.com		187.245.185.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:16.510293007 CEST	8.8.8.8	192.168.2.3	0xd095	No error (0)	colisumy.com		211.119.84.111	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:16.510293007 CEST	8.8.8.8	192.168.2.3	0xd095	No error (0)	colisumy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:16.510293007 CEST	8.8.8.8	192.168.2.3	0xd095	No error (0)	colisumy.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:16.671541929 CEST	8.8.8.8	192.168.2.3	0xca04	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:17.017462015 CEST	8.8.8.8	192.168.2.3	0x450d	No error (0)	colisumy.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:17.017462015 CEST	8.8.8.8	192.168.2.3	0x450d	No error (0)	colisumy.com		211.171.233.129	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:17.017462015 CEST	8.8.8.8	192.168.2.3	0x450d	No error (0)	colisumy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:17.017462015 CEST	8.8.8.8	192.168.2.3	0x450d	No error (0)	colisumy.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:17.017462015 CEST	8.8.8.8	192.168.2.3	0x450d	No error (0)	colisumy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:17.017462015 CEST	8.8.8.8	192.168.2.3	0x450d	No error (0)	colisumy.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:17.017462015 CEST	8.8.8.8	192.168.2.3	0x450d	No error (0)	colisumy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:17.017462015 CEST	8.8.8.8	192.168.2.3	0x450d	No error (0)	colisumy.com		187.245.185.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:17.017462015 CEST	8.8.8.8	192.168.2.3	0x450d	No error (0)	colisumy.com		211.119.84.111	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:17.017462015 CEST	8.8.8.8	192.168.2.3	0x450d	No error (0)	colisumy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:18.501964092 CEST	8.8.8.8	192.168.2.3	0x1f9b	No error (0)	potunulit.org		188.114.97.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:18.501964092 CEST	8.8.8.8	192.168.2.3	0x1f9b	No error (0)	potunulit.org		188.114.96.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:18.790283918 CEST	8.8.8.8	192.168.2.3	0x2085	No error (0)	colisumy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:18.790283918 CEST	8.8.8.8	192.168.2.3	0x2085	No error (0)	colisumy.com		187.245.185.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:18.790283918 CEST	8.8.8.8	192.168.2.3	0x2085	No error (0)	colisumy.com		211.119.84.111	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:18.790283918 CEST	8.8.8.8	192.168.2.3	0x2085	No error (0)	colisumy.com		183.100.39.157	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:18.790283918 CEST	8.8.8.8	192.168.2.3	0x2085	No error (0)	colisumy.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:18.790283918 CEST	8.8.8.8	192.168.2.3	0x2085	No error (0)	colisumy.com		211.171.233.129	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:18.790283918 CEST	8.8.8.8	192.168.2.3	0x2085	No error (0)	colisumy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:18.790283918 CEST	8.8.8.8	192.168.2.3	0x2085	No error (0)	colisumy.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:18.790283918 CEST	8.8.8.8	192.168.2.3	0x2085	No error (0)	colisumy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:18.790283918 CEST	8.8.8.8	192.168.2.3	0x2085	No error (0)	colisumy.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:19.477701902 CEST	8.8.8.8	192.168.2.3	0x3028	No error (0)	adsmanager.facebook.com	star.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
May 28, 2023 10:43:19.477701902 CEST	8.8.8.8	192.168.2.3	0x3028	No error (0)	star.facebook.com	star.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
May 28, 2023 10:43:19.477701902 CEST	8.8.8.8	192.168.2.3	0x3028	No error (0)	star.c10r.facebook.com		157.240.17.17	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:19.903872013 CEST	8.8.8.8	192.168.2.3	0x1826	No error (0)	zexeq.com		5.163.228.78	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:19.903872013 CEST	8.8.8.8	192.168.2.3	0x1826	No error (0)	zexeq.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:19.903872013 CEST	8.8.8.8	192.168.2.3	0x1826	No error (0)	zexeq.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:19.903872013 CEST	8.8.8.8	192.168.2.3	0x1826	No error (0)	zexeq.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:19.903872013 CEST	8.8.8.8	192.168.2.3	0x1826	No error (0)	zexeq.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:19.903872013 CEST	8.8.8.8	192.168.2.3	0x1826	No error (0)	zexeq.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:19.903872013 CEST	8.8.8.8	192.168.2.3	0x1826	No error (0)	zexeq.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:19.903872013 CEST	8.8.8.8	192.168.2.3	0x1826	No error (0)	zexeq.com		211.59.14.90	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:19.903872013 CEST	8.8.8.8	192.168.2.3	0x1826	No error (0)	zexeq.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:19.903872013 CEST	8.8.8.8	192.168.2.3	0x1826	No error (0)	zexeq.com		2.180.10.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.248779058 CEST	8.8.8.8	192.168.2.3	0xad6c	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.248779058 CEST	8.8.8.8	192.168.2.3	0xad6c	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.248779058 CEST	8.8.8.8	192.168.2.3	0xad6c	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.248779058 CEST	8.8.8.8	192.168.2.3	0xad6c	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.248779058 CEST	8.8.8.8	192.168.2.3	0xad6c	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.248779058 CEST	8.8.8.8	192.168.2.3	0xad6c	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:20.248779058 CEST	8.8.8.8	192.168.2.3	0xad6c	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.248779058 CEST	8.8.8.8	192.168.2.3	0xad6c	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.248779058 CEST	8.8.8.8	192.168.2.3	0xad6c	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.248779058 CEST	8.8.8.8	192.168.2.3	0xad6c	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.732796907 CEST	8.8.8.8	192.168.2.3	0xa0b6	No error (0)	zexeq.com		5.163.228.78	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.732796907 CEST	8.8.8.8	192.168.2.3	0xa0b6	No error (0)	zexeq.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.732796907 CEST	8.8.8.8	192.168.2.3	0xa0b6	No error (0)	zexeq.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.732796907 CEST	8.8.8.8	192.168.2.3	0xa0b6	No error (0)	zexeq.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.732796907 CEST	8.8.8.8	192.168.2.3	0xa0b6	No error (0)	zexeq.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.732796907 CEST	8.8.8.8	192.168.2.3	0xa0b6	No error (0)	zexeq.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.732796907 CEST	8.8.8.8	192.168.2.3	0xa0b6	No error (0)	zexeq.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.732796907 CEST	8.8.8.8	192.168.2.3	0xa0b6	No error (0)	zexeq.com		211.59.14.90	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.732796907 CEST	8.8.8.8	192.168.2.3	0xa0b6	No error (0)	zexeq.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.732796907 CEST	8.8.8.8	192.168.2.3	0xa0b6	No error (0)	zexeq.com		2.180.10.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:20.846388102 CEST	8.8.8.8	192.168.2.3	0x9518	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
May 28, 2023 10:43:20.846388102 CEST	8.8.8.8	192.168.2.3	0x9518	No error (0)	star-mini.c10r.facebook.com		157.240.9.35	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.043874979 CEST	8.8.8.8	192.168.2.3	0x3f8a	No error (0)	potunulit.org		188.114.97.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.043874979 CEST	8.8.8.8	192.168.2.3	0x3f8a	No error (0)	potunulit.org		188.114.96.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.132613897 CEST	8.8.8.8	192.168.2.3	0xe689	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.132613897 CEST	8.8.8.8	192.168.2.3	0xe689	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.132613897 CEST	8.8.8.8	192.168.2.3	0xe689	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.132613897 CEST	8.8.8.8	192.168.2.3	0xe689	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.132613897 CEST	8.8.8.8	192.168.2.3	0xe689	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.132613897 CEST	8.8.8.8	192.168.2.3	0xe689	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.132613897 CEST	8.8.8.8	192.168.2.3	0xe689	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:22.132613897 CEST	8.8.8.8	192.168.2.3	0xe689	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.132613897 CEST	8.8.8.8	192.168.2.3	0xe689	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.132613897 CEST	8.8.8.8	192.168.2.3	0xe689	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.417212963 CEST	8.8.8.8	192.168.2.3	0xa2d	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:22.796928883 CEST	8.8.8.8	192.168.2.3	0xe43	No error (0)	ss.apjeoighw.com		154.221.31.191	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:23.615879059 CEST	8.8.8.8	192.168.2.3	0x5e33	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:23.615879059 CEST	8.8.8.8	192.168.2.3	0x5e33	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:23.615879059 CEST	8.8.8.8	192.168.2.3	0x5e33	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:23.615879059 CEST	8.8.8.8	192.168.2.3	0x5e33	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:23.615879059 CEST	8.8.8.8	192.168.2.3	0x5e33	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:23.615879059 CEST	8.8.8.8	192.168.2.3	0x5e33	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:23.615879059 CEST	8.8.8.8	192.168.2.3	0x5e33	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:23.615879059 CEST	8.8.8.8	192.168.2.3	0x5e33	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:23.615879059 CEST	8.8.8.8	192.168.2.3	0x5e33	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:23.615879059 CEST	8.8.8.8	192.168.2.3	0x5e33	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:23.970146894 CEST	8.8.8.8	192.168.2.3	0x4fc2	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:24.216830015 CEST	8.8.8.8	192.168.2.3	0x30c4	No error (0)	colisumy.com		211.171.233.129	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:24.216830015 CEST	8.8.8.8	192.168.2.3	0x30c4	No error (0)	colisumy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:24.216830015 CEST	8.8.8.8	192.168.2.3	0x30c4	No error (0)	colisumy.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:24.216830015 CEST	8.8.8.8	192.168.2.3	0x30c4	No error (0)	colisumy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:24.216830015 CEST	8.8.8.8	192.168.2.3	0x30c4	No error (0)	colisumy.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:24.216830015 CEST	8.8.8.8	192.168.2.3	0x30c4	No error (0)	colisumy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:24.216830015 CEST	8.8.8.8	192.168.2.3	0x30c4	No error (0)	colisumy.com		187.245.185.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:24.216830015 CEST	8.8.8.8	192.168.2.3	0x30c4	No error (0)	colisumy.com		211.119.84.111	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:24.216830015 CEST	8.8.8.8	192.168.2.3	0x30c4	No error (0)	colisumy.com		183.100.39.157	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:24.216830015 CEST	8.8.8.8	192.168.2.3	0x30c4	No error (0)	colisumy.com		211.119.84.112	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:25.163640022 CEST	8.8.8.8	192.168.2.3	0x5cc3	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:25.163640022 CEST	8.8.8.8	192.168.2.3	0x5cc3	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:25.163640022 CEST	8.8.8.8	192.168.2.3	0x5cc3	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:25.163640022 CEST	8.8.8.8	192.168.2.3	0x5cc3	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:25.163640022 CEST	8.8.8.8	192.168.2.3	0x5cc3	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:25.163640022 CEST	8.8.8.8	192.168.2.3	0x5cc3	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:25.163640022 CEST	8.8.8.8	192.168.2.3	0x5cc3	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:25.163640022 CEST	8.8.8.8	192.168.2.3	0x5cc3	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:25.163640022 CEST	8.8.8.8	192.168.2.3	0x5cc3	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:25.163640022 CEST	8.8.8.8	192.168.2.3	0x5cc3	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:26.496707916 CEST	8.8.8.8	192.168.2.3	0x36ac	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:26.496707916 CEST	8.8.8.8	192.168.2.3	0x36ac	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:26.496707916 CEST	8.8.8.8	192.168.2.3	0x36ac	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:26.496707916 CEST	8.8.8.8	192.168.2.3	0x36ac	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:26.496707916 CEST	8.8.8.8	192.168.2.3	0x36ac	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:26.496707916 CEST	8.8.8.8	192.168.2.3	0x36ac	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:26.496707916 CEST	8.8.8.8	192.168.2.3	0x36ac	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:26.496707916 CEST	8.8.8.8	192.168.2.3	0x36ac	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:26.496707916 CEST	8.8.8.8	192.168.2.3	0x36ac	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:26.496707916 CEST	8.8.8.8	192.168.2.3	0x36ac	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:28.035729885 CEST	8.8.8.8	192.168.2.3	0xbebf	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:28.035729885 CEST	8.8.8.8	192.168.2.3	0xbebf	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:28.035729885 CEST	8.8.8.8	192.168.2.3	0xbebf	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:28.035729885 CEST	8.8.8.8	192.168.2.3	0xbebf	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:28.035729885 CEST	8.8.8.8	192.168.2.3	0xbebf	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:28.035729885 CEST	8.8.8.8	192.168.2.3	0xbebf	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:28.035729885 CEST	8.8.8.8	192.168.2.3	0xbebf	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:28.035729885 CEST	8.8.8.8	192.168.2.3	0xbebf	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:28.035729885 CEST	8.8.8.8	192.168.2.3	0xbebf	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:28.035729885 CEST	8.8.8.8	192.168.2.3	0xbebf	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:29.543556929 CEST	8.8.8.8	192.168.2.3	0xf4f1	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:29.543556929 CEST	8.8.8.8	192.168.2.3	0xf4f1	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:29.543556929 CEST	8.8.8.8	192.168.2.3	0xf4f1	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:29.543556929 CEST	8.8.8.8	192.168.2.3	0xf4f1	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:29.543556929 CEST	8.8.8.8	192.168.2.3	0xf4f1	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:29.543556929 CEST	8.8.8.8	192.168.2.3	0xf4f1	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:29.543556929 CEST	8.8.8.8	192.168.2.3	0xf4f1	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:29.543556929 CEST	8.8.8.8	192.168.2.3	0xf4f1	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:29.543556929 CEST	8.8.8.8	192.168.2.3	0xf4f1	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:29.543556929 CEST	8.8.8.8	192.168.2.3	0xf4f1	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:30.479723930 CEST	8.8.8.8	192.168.2.3	0x7f	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:30.909862995 CEST	8.8.8.8	192.168.2.3	0x89c9	No error (0)	zexeq.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:30.909862995 CEST	8.8.8.8	192.168.2.3	0x89c9	No error (0)	zexeq.com		2.180.10.7	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:30.909862995 CEST	8.8.8.8	192.168.2.3	0x89c9	No error (0)	zexeq.com		5.163.228.78	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:30.909862995 CEST	8.8.8.8	192.168.2.3	0x89c9	No error (0)	zexeq.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:30.909862995 CEST	8.8.8.8	192.168.2.3	0x89c9	No error (0)	zexeq.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:30.909862995 CEST	8.8.8.8	192.168.2.3	0x89c9	No error (0)	zexeq.com		211.40.39.251	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:30.909862995 CEST	8.8.8.8	192.168.2.3	0x89c9	No error (0)	zexeq.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:30.909862995 CEST	8.8.8.8	192.168.2.3	0x89c9	No error (0)	zexeq.com		211.119.84.112	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:30.909862995 CEST	8.8.8.8	192.168.2.3	0x89c9	No error (0)	zexeq.com		201.124.33.177	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:30.909862995 CEST	8.8.8.8	192.168.2.3	0x89c9	No error (0)	zexeq.com		211.59.14.90	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:31.201472044 CEST	8.8.8.8	192.168.2.3	0xc813	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:31.201472044 CEST	8.8.8.8	192.168.2.3	0xc813	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:31.201472044 CEST	8.8.8.8	192.168.2.3	0xc813	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:31.201472044 CEST	8.8.8.8	192.168.2.3	0xc813	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:31.201472044 CEST	8.8.8.8	192.168.2.3	0xc813	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:31.201472044 CEST	8.8.8.8	192.168.2.3	0xc813	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:31.201472044 CEST	8.8.8.8	192.168.2.3	0xc813	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:31.201472044 CEST	8.8.8.8	192.168.2.3	0xc813	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:31.201472044 CEST	8.8.8.8	192.168.2.3	0xc813	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:31.201472044 CEST	8.8.8.8	192.168.2.3	0xc813	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:31.590174913 CEST	8.8.8.8	192.168.2.3	0xea73	No error (0)	adsmanager.facebook.com	star.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
May 28, 2023 10:43:31.590174913 CEST	8.8.8.8	192.168.2.3	0xea73	No error (0)	star.facebook.com	star.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
May 28, 2023 10:43:31.590174913 CEST	8.8.8.8	192.168.2.3	0xea73	No error (0)	star.c10r.facebook.com		157.240.17.17	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:32.185162067 CEST	8.8.8.8	192.168.2.3	0x72a9	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
May 28, 2023 10:43:32.185162067 CEST	8.8.8.8	192.168.2.3	0x72a9	No error (0)	star-mini.c10r.facebook.com		157.240.9.35	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:32.495310068 CEST	8.8.8.8	192.168.2.3	0x5905	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:32.495310068 CEST	8.8.8.8	192.168.2.3	0x5905	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:32.495310068 CEST	8.8.8.8	192.168.2.3	0x5905	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:32.495310068 CEST	8.8.8.8	192.168.2.3	0x5905	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:32.495310068 CEST	8.8.8.8	192.168.2.3	0x5905	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:32.495310068 CEST	8.8.8.8	192.168.2.3	0x5905	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:32.495310068 CEST	8.8.8.8	192.168.2.3	0x5905	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:32.495310068 CEST	8.8.8.8	192.168.2.3	0x5905	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:32.495310068 CEST	8.8.8.8	192.168.2.3	0x5905	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:32.495310068 CEST	8.8.8.8	192.168.2.3	0x5905	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:33.652901888 CEST	8.8.8.8	192.168.2.3	0x4431	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:34.496217012 CEST	8.8.8.8	192.168.2.3	0x75e7	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:34.496217012 CEST	8.8.8.8	192.168.2.3	0x75e7	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:34.496217012 CEST	8.8.8.8	192.168.2.3	0x75e7	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:34.496217012 CEST	8.8.8.8	192.168.2.3	0x75e7	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:34.496217012 CEST	8.8.8.8	192.168.2.3	0x75e7	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:34.496217012 CEST	8.8.8.8	192.168.2.3	0x75e7	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:34.496217012 CEST	8.8.8.8	192.168.2.3	0x75e7	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:34.496217012 CEST	8.8.8.8	192.168.2.3	0x75e7	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:34.496217012 CEST	8.8.8.8	192.168.2.3	0x75e7	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:34.496217012 CEST	8.8.8.8	192.168.2.3	0x75e7	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:36.019514084 CEST	8.8.8.8	192.168.2.3	0x64e9	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:36.019514084 CEST	8.8.8.8	192.168.2.3	0x64e9	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:36.019514084 CEST	8.8.8.8	192.168.2.3	0x64e9	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:36.019514084 CEST	8.8.8.8	192.168.2.3	0x64e9	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:36.019514084 CEST	8.8.8.8	192.168.2.3	0x64e9	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:36.019514084 CEST	8.8.8.8	192.168.2.3	0x64e9	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:36.019514084 CEST	8.8.8.8	192.168.2.3	0x64e9	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:36.019514084 CEST	8.8.8.8	192.168.2.3	0x64e9	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:36.019514084 CEST	8.8.8.8	192.168.2.3	0x64e9	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:36.019514084 CEST	8.8.8.8	192.168.2.3	0x64e9	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:37.228518963 CEST	8.8.8.8	192.168.2.3	0x6cdd	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:37.259345055 CEST	8.8.8.8	192.168.2.3	0x5481	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:37.259345055 CEST	8.8.8.8	192.168.2.3	0x5481	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:37.259345055 CEST	8.8.8.8	192.168.2.3	0x5481	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:37.259345055 CEST	8.8.8.8	192.168.2.3	0x5481	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:37.259345055 CEST	8.8.8.8	192.168.2.3	0x5481	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:37.259345055 CEST	8.8.8.8	192.168.2.3	0x5481	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:37.259345055 CEST	8.8.8.8	192.168.2.3	0x5481	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:37.259345055 CEST	8.8.8.8	192.168.2.3	0x5481	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:37.259345055 CEST	8.8.8.8	192.168.2.3	0x5481	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:37.259345055 CEST	8.8.8.8	192.168.2.3	0x5481	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:38.797343016 CEST	8.8.8.8	192.168.2.3	0xa202	No error (0)	shsplatform.co.uk		80.66.203.53	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:39.436762094 CEST	8.8.8.8	192.168.2.3	0xa76c	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:39.436762094 CEST	8.8.8.8	192.168.2.3	0xa76c	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:39.436762094 CEST	8.8.8.8	192.168.2.3	0xa76c	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:39.436762094 CEST	8.8.8.8	192.168.2.3	0xa76c	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:39.436762094 CEST	8.8.8.8	192.168.2.3	0xa76c	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:39.436762094 CEST	8.8.8.8	192.168.2.3	0xa76c	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:39.436762094 CEST	8.8.8.8	192.168.2.3	0xa76c	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:39.436762094 CEST	8.8.8.8	192.168.2.3	0xa76c	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:39.436762094 CEST	8.8.8.8	192.168.2.3	0xa76c	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:39.436762094 CEST	8.8.8.8	192.168.2.3	0xa76c	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:40.787662029 CEST	8.8.8.8	192.168.2.3	0xcb14	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:40.787662029 CEST	8.8.8.8	192.168.2.3	0xcb14	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:40.787662029 CEST	8.8.8.8	192.168.2.3	0xcb14	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:40.787662029 CEST	8.8.8.8	192.168.2.3	0xcb14	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:40.787662029 CEST	8.8.8.8	192.168.2.3	0xcb14	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:40.787662029 CEST	8.8.8.8	192.168.2.3	0xcb14	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:40.787662029 CEST	8.8.8.8	192.168.2.3	0xcb14	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:40.787662029 CEST	8.8.8.8	192.168.2.3	0xcb14	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:40.787662029 CEST	8.8.8.8	192.168.2.3	0xcb14	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:40.787662029 CEST	8.8.8.8	192.168.2.3	0xcb14	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:42.306963921 CEST	8.8.8.8	192.168.2.3	0xed1c	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:42.700331926 CEST	8.8.8.8	192.168.2.3	0xd5a1	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:42.700331926 CEST	8.8.8.8	192.168.2.3	0xd5a1	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:42.700331926 CEST	8.8.8.8	192.168.2.3	0xd5a1	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:42.700331926 CEST	8.8.8.8	192.168.2.3	0xd5a1	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:42.700331926 CEST	8.8.8.8	192.168.2.3	0xd5a1	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:42.700331926 CEST	8.8.8.8	192.168.2.3	0xd5a1	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:42.700331926 CEST	8.8.8.8	192.168.2.3	0xd5a1	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:42.700331926 CEST	8.8.8.8	192.168.2.3	0xd5a1	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:42.700331926 CEST	8.8.8.8	192.168.2.3	0xd5a1	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:42.700331926 CEST	8.8.8.8	192.168.2.3	0xd5a1	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:44.234476089 CEST	8.8.8.8	192.168.2.3	0xba0a	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:44.234476089 CEST	8.8.8.8	192.168.2.3	0xba0a	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:44.234476089 CEST	8.8.8.8	192.168.2.3	0xba0a	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:44.234476089 CEST	8.8.8.8	192.168.2.3	0xba0a	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:44.234476089 CEST	8.8.8.8	192.168.2.3	0xba0a	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:44.234476089 CEST	8.8.8.8	192.168.2.3	0xba0a	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:44.234476089 CEST	8.8.8.8	192.168.2.3	0xba0a	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:44.234476089 CEST	8.8.8.8	192.168.2.3	0xba0a	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:44.234476089 CEST	8.8.8.8	192.168.2.3	0xba0a	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:44.234476089 CEST	8.8.8.8	192.168.2.3	0xba0a	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:45.761905909 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:45.761905909 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:45.761905909 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:45.761905909 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:45.761905909 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:45.761905909 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:45.761905909 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:45.761905909 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:45.761905909 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:45.761905909 CEST	8.8.8.8	192.168.2.3	0x8d9d	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:46.985579014 CEST	8.8.8.8	192.168.2.3	0xef30	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:46.985579014 CEST	8.8.8.8	192.168.2.3	0xef30	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:46.985579014 CEST	8.8.8.8	192.168.2.3	0xef30	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:46.985579014 CEST	8.8.8.8	192.168.2.3	0xef30	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:46.985579014 CEST	8.8.8.8	192.168.2.3	0xef30	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:46.985579014 CEST	8.8.8.8	192.168.2.3	0xef30	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:46.985579014 CEST	8.8.8.8	192.168.2.3	0xef30	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:46.985579014 CEST	8.8.8.8	192.168.2.3	0xef30	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:46.985579014 CEST	8.8.8.8	192.168.2.3	0xef30	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:46.985579014 CEST	8.8.8.8	192.168.2.3	0xef30	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:47.364337921 CEST	8.8.8.8	192.168.2.3	0xb441	No error (0)	adsmanager.facebook.com	star.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
May 28, 2023 10:43:47.364337921 CEST	8.8.8.8	192.168.2.3	0xb441	No error (0)	star.facebook.com	star.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
May 28, 2023 10:43:47.364337921 CEST	8.8.8.8	192.168.2.3	0xb441	No error (0)	star.c10r.facebook.com		157.240.17.17	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:47.384660006 CEST	8.8.8.8	192.168.2.3	0x6476	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:47.877331018 CEST	8.8.8.8	192.168.2.3	0xaa8d	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
May 28, 2023 10:43:47.877331018 CEST	8.8.8.8	192.168.2.3	0xaa8d	No error (0)	star-mini.c10r.facebook.com		157.240.9.35	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:48.646327019 CEST	8.8.8.8	192.168.2.3	0xfe12	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:48.646327019 CEST	8.8.8.8	192.168.2.3	0xfe12	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:48.646327019 CEST	8.8.8.8	192.168.2.3	0xfe12	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:48.646327019 CEST	8.8.8.8	192.168.2.3	0xfe12	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:48.646327019 CEST	8.8.8.8	192.168.2.3	0xfe12	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:48.646327019 CEST	8.8.8.8	192.168.2.3	0xfe12	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:48.646327019 CEST	8.8.8.8	192.168.2.3	0xfe12	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:48.646327019 CEST	8.8.8.8	192.168.2.3	0xfe12	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:48.646327019 CEST	8.8.8.8	192.168.2.3	0xfe12	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:48.646327019 CEST	8.8.8.8	192.168.2.3	0xfe12	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:50.074316025 CEST	8.8.8.8	192.168.2.3	0x6bb1	No error (0)	ss.apjeoighw.com		154.221.31.191	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:50.150230885 CEST	8.8.8.8	192.168.2.3	0x2973	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:50.150230885 CEST	8.8.8.8	192.168.2.3	0x2973	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:50.150230885 CEST	8.8.8.8	192.168.2.3	0x2973	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:50.150230885 CEST	8.8.8.8	192.168.2.3	0x2973	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:50.150230885 CEST	8.8.8.8	192.168.2.3	0x2973	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:50.150230885 CEST	8.8.8.8	192.168.2.3	0x2973	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:50.150230885 CEST	8.8.8.8	192.168.2.3	0x2973	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:50.150230885 CEST	8.8.8.8	192.168.2.3	0x2973	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:50.150230885 CEST	8.8.8.8	192.168.2.3	0x2973	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:50.150230885 CEST	8.8.8.8	192.168.2.3	0x2973	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:51.665191889 CEST	8.8.8.8	192.168.2.3	0x2561	No error (0)	toobussy.com		222.236.49.123	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:51.665191889 CEST	8.8.8.8	192.168.2.3	0x2561	No error (0)	toobussy.com		175.119.10.231	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:43:51.665191889 CEST	8.8.8.8	192.168.2.3	0x2561	No error (0)	toobussy.com		123.140.161.243	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:51.665191889 CEST	8.8.8.8	192.168.2.3	0x2561	No error (0)	toobussy.com		37.34.248.24	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:51.665191889 CEST	8.8.8.8	192.168.2.3	0x2561	No error (0)	toobussy.com		80.210.25.252	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:51.665191889 CEST	8.8.8.8	192.168.2.3	0x2561	No error (0)	toobussy.com		222.236.49.124	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:51.665191889 CEST	8.8.8.8	192.168.2.3	0x2561	No error (0)	toobussy.com		109.98.58.98	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:51.665191889 CEST	8.8.8.8	192.168.2.3	0x2561	No error (0)	toobussy.com		175.126.109.15	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:51.665191889 CEST	8.8.8.8	192.168.2.3	0x2561	No error (0)	toobussy.com		175.120.254.9	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:51.665191889 CEST	8.8.8.8	192.168.2.3	0x2561	No error (0)	toobussy.com		183.100.39.157	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:52.439465046 CEST	8.8.8.8	192.168.2.3	0xcfb6	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:57.183255911 CEST	8.8.8.8	192.168.2.3	0xb748	No error (0)	adsmanager.facebook.com	star.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
May 28, 2023 10:43:57.183255911 CEST	8.8.8.8	192.168.2.3	0xb748	No error (0)	star.facebook.com	star.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
May 28, 2023 10:43:57.183255911 CEST	8.8.8.8	192.168.2.3	0xb748	No error (0)	star.c10r.facebook.com		157.240.17.17	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:57.786288977 CEST	8.8.8.8	192.168.2.3	0x9b9b	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
May 28, 2023 10:43:57.786288977 CEST	8.8.8.8	192.168.2.3	0x9b9b	No error (0)	star-mini.c10r.facebook.com		157.240.234.35	A (IP address)	IN (0x0001)	false
May 28, 2023 10:43:59.847691059 CEST	8.8.8.8	192.168.2.3	0xdec8	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false
May 28, 2023 10:44:04.979201078 CEST	8.8.8.8	192.168.2.3	0x92cb	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- speedlab.com.eg
- api.2ip.ua
- t.me
- adsmanager.facebook.com
- www.facebook.com
- shsplatform.co.uk
- xlqkimn.org
  - potunulit.org
- mxltwpsqeo.net
- colisumy.com

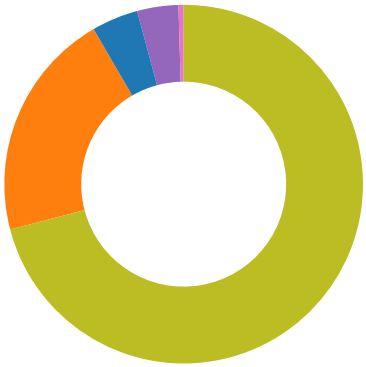
- csusaymthn.com
- iviost.org
- wkqar.net
- dudvlk.com
- 45.9.74.80
- zexeq.com
- qqiuoruppq.com
- ybcrbcpvym.com
- jp.imgjeoighw.com
- negwl.net
- sfmvlnbt.com
- mbwheantep.net
- ajoab.net
- wjhcfonfk.org
- ipame.net
- bxpeemr.org
- kxvorcn.com
- pppdb.org
- shwsp.org
- 188.34.154.187:30303
- vyuaut.com
- waofgmma.org
- gtnvc.net
- lfcxfryvi.com
- tcovw.org
- dpvseurycv.org
- oqqtqnj.org
- ykcanuky.org
- wuwnf.net
- yyabnclq.com

- dyrfgkau.org
- uytll.net
- cxhhlcn.com
- laydyxa.com
- oluqgvm.org
- lugojs.net
- aomtmlmpuh.org
- cfjtxu.com
- sbcht.com
  - toobussy.com
- akimoe.net
- dlaxujokn.org
- ss.apjeoighw.com
- dmcdswi.net
- fgfsyqph.org
- xmewqwgqx.org
- dsoav.org
- ollfl.org
- ylfleydl.org
- etftmd.org
- 194.180.48.90
- fglqosxf.org
- qlcjnrapy.net
- fatvkcvmxq.net
- vacsrkw.com
- cdgmadwmn.net
- vplsfigg.com
- doqsqrp.net
- nypsigtije.net
- wjgjontf.org

- atqoikuxkw.net
- octqh.com
- xgeaptg.net

Statistics

Behavior



- 01860199.exe
- explorer.exe
- hwgujdv
- D804.exe
- D804.exe
- C861.exe
- icacls.exe
- WerFault.exe
- WerFault.exe
- D804.exe
- D804.exe
- D804.exe
- D804.exe
- 3C54.exe
- aafg31.exe
- NewPlayer.exe
- XandETC.exe
- build2.exe
- B46F.exe
- B46F.exe
- A170.exe
- D804.exe
- A170.exe
- build3.exe
- D804.exe
- build2.exe
- schtasks.exe
- 913F.exe
- mnolyk.exe
- conhost.exe
- 913F.exe
- F4F7.exe
- mstsca.exe
- 5DA0.exe

Click to jump to process

System Behavior

Analysis Process: 01860199.exe PID: **1264**, Parent PID: **3452**

General

Target ID:	0
Start time:	10:41:55
Start date:	28/05/2023
Path:	C:\Users\user\Desktop\01860199.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\01860199.exe
Imagebase:	0x400000
File size:	289280 bytes
MD5 hash:	3D8207E1CE6762FF10DB118BEE3BD99B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.380036043.0000000000859000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.380148014.0000000002421000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.380148014.0000000002421000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.380129580.0000000002400000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.380129580.0000000002400000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.380107918.00000000023F0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3452**, Parent PID: **1264**

General

Target ID:	1
Start time:	10:42:01
Start date:	28/05/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69fe90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\hwgujdv	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	5802156	CopyFileW
C:\Users\user\AppData\Roaming\hwgujdv\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	5802156	CopyFileW
C:\Users\user\AppData\Local\Temp\D804.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\D804.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\C861.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\C861.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\3C54.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\3C54.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\B46F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B46F.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\A170.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\A170.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\913F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\913F.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\F4F7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\F4F7.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\5DA0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\5DA0.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\CBE6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\CBE6.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\B8C8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\B8C8.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\A3D5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\A3D5.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\673.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\673.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\6FA9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\6FA9.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\EA44.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\EA44.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\D689.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\D689.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\388B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\388B.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\9F31.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\9F31.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Roaming\ewgujdv	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	5932003	CopyFileW
C:\Users\user\AppData\Local\Temp\BC2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5802BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\BC2.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5802C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\57DC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5932A56	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\57DC.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5932B1A	CreateFileW
C:\Users\user\AppData\Local\Temp\3E02.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5932A56	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\3E02.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5932B1A	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\01860199.exe	success or wait	1	5802167	DeleteFileW
C:\Users\user\AppData\Roaming\hwgujdv:Zone.Identifier	success or wait	1	58021B2	DeleteFileW
C:\Users\user\AppData\Local\Temp\D804.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\C861.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\3C54.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\B46F.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\A170.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\913F.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\F4F7.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\5DA0.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\CBE6.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\B8C8.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\A3D5.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\673.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\6FA9.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\EA44.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\D689.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\388B.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\9F31.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\F4F7.exe	success or wait	1	5932014	DeleteFileW
C:\Users\user\AppData\Local\Temp\BC2.tmp	success or wait	1	5802BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\57DC.tmp	success or wait	1	5932A5F	DeleteFileW
C:\Users\user\AppData\Local\Temp\3E02.tmp	success or wait	1	5932A5F	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\hwgujdv	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 65 fd fd 63 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPELec	success or wait	3	5802156	CopyFileW
C:\Users\user\AppData\Roaming\hwgujdv:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	5802156	CopyFileW
C:\Users\user\AppData\Local\Temp\D804.exe	0	802304	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 34 fd 61 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPEL4a	success or wait	1	5802CA0	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\C861.exe</td><td>0</td><td>288768</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 47 fd 0e 63 00 00 00 00 00 00 00 fd 00 02</td><td>MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPELGc</td><td>success or wait</td><td>1</td><td>5802CA0</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\3C54.exe</td><td>0</td><td>5129728</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd 70 64 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0b 00 00 3c 4e 00 00 08 00 00 00 00 00 00 fd 5a 4e 00 00 20 00 00 00 60 4e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 4e 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00</td><td>MZ@!L!This program cannot be run in DOS mode.$PELpd<NZN `N@N@</td><td>success or wait</td><td>1</td><td>5802CA0</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B46F.exe	0	802304	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 34 fd 61 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPEL4a	success or wait	1	5802CA0	WriteFile
C:\Users\user\AppData\Local\Temp\A170.exe	0	809984	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 96 62 00 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 4c 0a	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPELbL	success or wait	1	5802CA0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\913F.exe	0	809984	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 96 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 4c 0a	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPELbL	success or wait	1	5802CA0	WriteFile
C:\Users\user\AppData\Local\Temp\F4F7.exe	0	288768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 47 fd 0e 63 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPELGc	success or wait	1	5802CA0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5DA0.exe	0	5129728	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd 70 64 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0b 00 00 3c 4e 00 00 08 00 00 00 00 00 00 fd 5a 4e 00 00 20 00 00 00 60 4e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 4e 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELpd<NZN `N@N@	success or wait	1	5802CA0	WriteFile
C:\Users\user\AppData\Local\Temp\CBE6.exe	0	802304	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 34 fd 61 00 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPEL4a	success or wait	1	5802CA0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B8C8.exe	0	809984	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 96 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 4c 0a	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPELbL	success or wait	1	5802CA0	WriteFile
C:\Users\user\AppData\Local\Temp\A3D5.exe	0	809984	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 96 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 4c 0a	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPELbL	success or wait	1	5802CA0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\673.exe	0	288768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 47 fd 0e 63 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPELGc	success or wait	1	5802CA0	WriteFile
C:\Users\user\AppData\Local\Temp\6FA9.exe	0	5129728	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd 70 64 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0b 00 00 3c 4e 00 00 08 00 00 00 00 00 00 fd 5a 4e 00 00 20 00 00 00 60 4e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 4e 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELpd<NZN `N@ N@	success or wait	1	5802CA0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\EA44.exe	0	802304	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 34 fd 61 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPEL4a	success or wait	1	5802CA0	WriteFile
C:\Users\user\AppData\Local\Temp\D689.exe	0	809984	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 96 62 00 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 4c 0a	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPELbL	success or wait	1	5802CA0	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\388B.exe</td><td>0</td><td>288768</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 47 fd 0e 63 00 00 00 00 00 00 00 00 fd 00 02</td><td>MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c |c|cRichbPELGc</td><td>success or wait</td><td>1</td><td>5802CA0</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\9F31.exe</td><td>0</td><td>5129728</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd 70 64 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0b 00 00 3c 4e 00 00 08 00 00 00 00 00 00 fd 5a 4e 00 00 20 00 00 00 60 4e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 4e 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00</td><td>MZ@!L!This program cannot be run in DOS mode.$PELpd<NZN `N@ N@</td><td>success or wait</td><td>1</td><td>5802CA0</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ewgujdv	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 47 fd 0e 63 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPELGc	success or wait	3	5932003	CopyFileW
C:\Users\user\AppData\Local\Temp\BC2.exe	0	802304	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 34 fd 61 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPEL4a	success or wait	1	5802CA0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\57DC.exe	0	503808	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd 70 62 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPELpb	success or wait	1	5932B40	WriteFile
C:\Users\user\AppData\Local\Temp\3E02.exe	0	599040	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 03 fd 61 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPELa	success or wait	1	5932B40	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: hwgujdv PID: **5940**, Parent PID: **1080**

General

Target ID:	4

Start time:	10:42:34
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Roaming\hwgujdv
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\hwgujdv
Imagebase:	0x400000
File size:	289280 bytes
MD5 hash:	3D8207E1CE6762FF10DB118BEE3BD99B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000004.00000002.445989950.0000000000738000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000002.445573902.0000000000700000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000004.00000002.445573902.0000000000700000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000004.00000002.445509996.00000000006F0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000002.446406704.00000000022D1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000004.00000002.446406704.00000000022D1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 38%, ReversingLabs
Reputation:	low

Analysis Process: D804.exe PID: **2560**, Parent PID: **3452**

General

Target ID:	5
Start time:	10:42:37
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\D804.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\D804.exe
Imagebase:	0x400000
File size:	802304 bytes
MD5 hash:	6944FCA258A9009F9D3B7212CDB4874D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000005.00000002.442867169.0000000002690000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000005.00000002.442867169.0000000002690000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000005.00000002.442702951.00000000024A5000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: D804.exe PID: **772**, Parent PID: **2560**

General

Target ID:	6
Start time:	10:42:37
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\D804.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\D804.exe
Imagebase:	0x400000
File size:	802304 bytes
MD5 hash:	6944FCA258A9009F9D3B7212CDB4874D
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000006.00000002.449975040.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000006.00000002.449975040.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000006.00000002.449975040.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000006.00000002.449975040.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	411F94	CreateDirectoryW
C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	412052	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 26 fd fd fd 62 fd fd fd 62 fd fd fd 62 fd fd fd 7c fd 0d fd 7f fd fd fd 7c fd 1b fd 18 fd fd fd 7c fd 1c fd 48 fd fd fd 45 58 fd fd 6b fd fd fd 62 fd fd fd 98 fd 7c fd 12 fd 63 fd fd fd 7c fd 0c fd 63 fd fd fd 7c fd 09 fd 63 fd fd fd 52 69 63 68 62 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 34 fd 61 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$&bbb|||HEXkb|c|c|cRichbPEL4a	success or wait	4	412052	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SysHelper	expand unicode	"C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe" --AutoStart	success or wait	1	4120F9	RegSetValueExW

Analysis Process: C861.exe PID: 68, Parent PID: 3452

General

Target ID:	7
Start time:	10:42:38

Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\C861.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\C861.exe
Imagebase:	0x400000
File size:	288768 bytes
MD5 hash:	7A8E3D000FBA0F5765B98E2D78EB9D12
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000007.00000002.460164953.0000000000800000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000007.00000002.460214856.0000000000838000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: icacls.exe PID: 4704, Parent PID: 772

General

Target ID:	9
Start time:	10:42:39
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	icacls "C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e" /deny *S-1-1-0:(OI)(CI)(DE,DC)
Imagebase:	0x310000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	83			invalid handle	1	311B0A	WriteFile
unknown	unknown	59			invalid handle	1	311B0A	WriteFile

Analysis Process: WerFault.exe PID: 1868, Parent PID: 2620

General

Target ID:	10
Start time:	10:42:39
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 508 -p 68 -ip 68
Imagebase:	0x1190000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: WerFault.exe PID: **5568**, Parent PID: **68**

General

Target ID:	11
Start time:	10:42:39
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 68 -s 520
Imagebase:	0x1190000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CA51717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86DE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86DE.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_C861.exe_ee73edd8fcc59e6e41b76bbadce78e8978345d94_81c5b0e7_15ae9ed9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_C861.exe_ee73edd8fcc59e6e41b76bbadce78e8978345d94_81c5b0e7_15ae9ed9\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CA4497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp	success or wait	1	6CA4497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86DE.tmp	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86DE.tmp.xml	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86DC.tmp.csv	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8815.tmp.txt	success or wait	1	6CA4497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 73 64 fd 05 12 00 00 00 00 00	MDMP sd	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	5944	6	00 00 00 00 00 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 38 17 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 44 00 00 00 fd fd 73 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 20 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UB8GenuineIntelWTDsd Pacific Standard TimePacific Daylight Time	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	6866	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd 19 00 fd 2c 40 00 00 00 40 00 fd 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 67 fd 00 00 23 00 00 00 46 02 01 00 fd fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++,@@g#F+	success or wait	1	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	1620	168	fd 08 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 67 fd 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 67 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 1a 00 00	gg	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	9730	20	0e 00 00 00 00 fd 3d 00 00 00 00 00 fd 04 00 00 fd 26 00 00	=&	success or wait	14	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	9958	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 48 17 fd 00 00 00 00 00 00 00 fd 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 74 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 fd fd fd 07 00 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 05 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@{wHywt{w0(Pm `fwPSwB	success or wait	13	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	24846	2336	fd fd fd fd fd fd fd fd fd fd fd 28 fd 19 00 fd fd fd fd 38 fd 19 00 10 21 fd 74 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd 44 00 00 00 fd fd fd fd fd fd fd 00 00 40 00 fd fd fd fd 00 00 40 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 fd fd 19 00 fd 40 09 74 fd fd fd fd fd fd fd fd fd 19 00 fd 0b 77 fd fd 19 00 fd fd fd fd 60 fd fd 74 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 54 0b 77 fd fd 19 00 fd fd 19 00 fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd	(8!tD@@@tw`tTw	success or wait	1	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	7582	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd 19 00 fd 2c 40 00 00 00 40 00 fd 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 67 fd 00 00 23 00 00 00 46 02 01 00 fd fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++,@@g#F+	success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	1888	48	40 00 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 3e 00 00 00 00 00 fd fd fd 00 00 00 00 00 3c 02 00 00 7e 5b 00 00 fd 02 00 00 36 23 00 00	@ ><~[6#	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	1948	4	1f 00 00 00		success or wait	31	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	5950	22	10 00 00 00 43 00 38 00 36 00 31 00 2e 00 65 00 78 00 65 00 00 00	C861.exe	success or wait	31	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	5192	752	00 00 6e 77 00 00 00 00 00 fd 00 00 0e 38 01 00 20 fd fd fd fd 1a 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 10 fd 02 00 00 00 00 00 50 0e 03 00 00 00 00 47 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 4c fd 03 00 00 00 00 00 fd 27 04 00 00 00 00 00 00 00 00 00 00 00 00 00 77 fd 1a 00 00 00 00 00 fd 33 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 63 52 05 00 00 00 00	nw8 BB? #@AZbPGL'w3@cR	success or wait	1	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	27182	7550	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8517.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 18 0d 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 02 26 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 14 00 00 fd 72 00 00 15 00 00 00 fd 01 00 00 fd 14 00 00 16 00 00 00 fd 00 00 00 fd 16 00 00	&T8Tr	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	964	26	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>68</Pid>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	990	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	994	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	998	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 43 00 38 00 36 00 31 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>C861.exe</ImageName>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1060	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1064	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1068	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 32 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000002</CmdLineSignature>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1158	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1162	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1166	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 34 00 30 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1408</Uptime>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1208	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1212	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1216	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1298	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1302	2	09 00		success or wait	2	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1306	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1358	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1362	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1366	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1410	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1414	2	09 00		success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1420	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 32 00 32 00 34 00 37 00 36 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>82247680</PeakVirtualSize>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1506	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1510	2	09 00		success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1516	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 32 00 32 00 34 00 33 00 35 00 38 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>82243584</VirtualSize>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1586	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1590	2	09 00		success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1596	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 33 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2335</PageFaultCount>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1670	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1674	2	09 00		success or wait	3	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1680	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 30 00 32 00 37 00 35 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>9027584</PeakWorkingSetSize>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1776	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1780	2	09 00		success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1786	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 30 00 32 00 37 00 35 00 38 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>9027584</WorkingSetSize>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1866	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1870	2	09 00		success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1876	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 37 00 35 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>157528</QuotaPeakPagedPoolUsage>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1990	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	1994	2	09 00		success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2000	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 37 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>157352</QuotaPagedPoolUsage>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2098	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2102	2	09 00		success or wait	3	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2108	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 37 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>37752</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2232	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2236	2	09 00		success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2242	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 36 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>37616</QuotaNonPagedPoolUsage>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2350	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2354	2	09 00		success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2360	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 39 00 31 00 39 00 38 00 37 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3919872</PagefileUsage>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2436	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2440	2	09 00		success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2446	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 39 00 32 00 33 00 39 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3923968</PeakPagefileUsage>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2538	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2542	2	09 00		success or wait	3	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2548	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 39 00 31 00 39 00 38 00 37 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3919872</PrivateUsage>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2620	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2624	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2628	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2674	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2678	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2682	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2722	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2762	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2766	2	09 00		success or wait	4	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2774	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2804	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2808	2	09 00		success or wait	4	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2816	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2886	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2890	2	09 00		success or wait	4	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2898	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2988	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	2992	2	09 00		success or wait	4	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3000	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 36 00 38 00 33 00 32 00 33 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6683239</Uptime>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3060	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3138	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3142	2	09 00		success or wait	4	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3150	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3202	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3206	2	09 00		success or wait	4	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3214	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3258	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3262	2	09 00		success or wait	5	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3272	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3376	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3450	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3454	2	09 00		success or wait	5	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3464	78	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 35 00 32 00 37 00 34 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>152747</PageFaultCount>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3542	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3546	2	09 00		success or wait	5	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3556	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 35 00 36 00 34 00 37 00 31 00 32 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>156471296</PeakWorkingSetSize>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3656	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3660	2	09 00		success or wait	5	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3670	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 39 00 30 00 39 00 34 00 34 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>149094400</WorkingSetSize>	success or wait	1	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3754	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3758	2	09 00		success or wait	5	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3768	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 39 00 30 00 31 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11901 76</QuotaPeakPagedPoolUsage>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3884	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3888	2	09 00		success or wait	5	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3898	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 37 00 32 00 34 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1172432</ QuotaPagedPoolUsage>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	3998	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4002	2	09 00		success or wait	5	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4012	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 39 00 35 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>17 9524</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4138	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4142	2	09 00		success or wait	5	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4152	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 36 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>90640< /QuotaNonPagedPoolUsage>	success or wait	1	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4260	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4264	2	09 00		success or wait	5	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4274	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 30 00 37 00 37 00 30 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4407705 6</PagefileUsage>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4352	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4356	2	09 00		success or wait	5	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4366	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 39 00 36 00 31 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>51 961856</P eakPagefileUsage>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4460	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4464	2	09 00		success or wait	5	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4474	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 30 00 37 00 37 00 30 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4407705 6</PrivateUsage>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4548	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4552	2	09 00		success or wait	4	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4560	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation >	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4606	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4610	2	09 00		success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4616	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	2	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4666	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4698	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4702	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4704	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4752	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4790	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4794	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4798	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4850	4	0d 00 0a 00		success or wait	9	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4854	2	09 00		success or wait	18	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	4858	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 43 00 38 00 36 00 31 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>C861.exe</Parameter0>	success or wait	9	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	5566	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	5570	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	5572	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	5612	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	5616	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	5618	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	5656	4	0d 00 0a 00		success or wait	6	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	5660	2	09 00		success or wait	12	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	5664	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6218	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6222	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6224	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6264	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6268	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6270	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6308	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6312	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6316	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6410	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6414	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6418	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 67 00 77 00 6b 00 69 00 77 00 75 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>gwkiwu, Inc.</SystemManufacturer>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6524	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6528	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6532	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 67 00 77 00 6b 00 69 00 77 00 75 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>gwkiwu7,1</SystemProductName>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6628	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6632	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6636	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6756	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6760	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6764	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 33 00 36 00 37 00 35 00 33 00 37 00 31 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1636753710</OSInstallDate>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6846	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6850	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6854	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6956	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6960	2	09 00		success or wait	2	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	6964	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7032	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7036	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7038	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7078	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7082	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7084	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7118	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7122	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7126	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7222	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7226	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7228	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7264	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7268	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7270	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7294	4	0d 00 0a 00		success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7298	2	09 00		success or wait	6	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7302	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>80000000</Flags>	success or wait	3	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7546	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7550	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7552	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7578	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7582	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7584	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 32 00 38 00 54 00 31 00 37 00 3a 00 34 00 32 00 3a 00 34 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-28T17:42:40Z">	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7684	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7688	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7692	254	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 35 00 30 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 35 00 30 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22 00 3e 00	<Process AsId="365" PID="68" UptimeMS="250" TimeSinceCreationMS="250" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1">	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7946	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7950	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7954	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7974	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7978	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	7980	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	8018	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	8022	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	8024	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	8062	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	8066	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	8070	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 64 00 38 00 33 00 37 00 33 00 33 00 62 00 2d 00 61 00 32 00 62 00 36 00 2d 00 34 00 66 00 38 00 62 00 2d 00 61 00 34 00 61 00 63 00 2d 00 66 00 39 00 34 00 33 00 61 00 34 00 63 00 64 00 36 00 65 00 63 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>5d83733b-a2b6-4f8b-a4ac-f943a4cd6ecc</Guid>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	8168	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	8172	2	09 00		success or wait	2	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	8176	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 32 00 38 00 54 00 31 00 37 00 3a 00 34 00 32 00 3a 00 34 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-05-28T17:42:40Z</CreationTime>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	8274	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	8278	2	09 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	8280	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	8320	4	0d 00 0a 00		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8670.tmp.WERInternalMetadata.xml	8324	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6CA4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86DE.tmp.xml	0	4680	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_C861.exe_ee73edd8fcc59e6e41b76bbadce78e8978345d94_81c5b0e7_15ae9ed9\Report.wer	0	2	fd fd		success or wait	1	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_C861.exe_ee73edd8fcc59e6e41b76bbadce78e8978345d94_81c5b0e7_15ae9ed9\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	158	6CA4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_C861.exe_ee73edd8fcc59e6e41b76bbadce78e8978345d94_81c5b0e7_15ae9ed9\Report.wer	10074	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 31 00 37 00 31 00 37 00 34 00 39 00 32 00 32 00 39 00	MetadataHash=-1171749229	success or wait	1	6CA4497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: D804.exe PID: **1340**, Parent PID: **1080**

General

Target ID:	13
Start time:	10:42:40
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe --Task
Imagebase:	0x400000
File size:	802304 bytes
MD5 hash:	6944FCA258A9009F9D3B7212CDB4874D
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000D.00000002.450548636.0000000002490000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000D.00000002.450667818.0000000002530000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000D.00000002.450667818.0000000002530000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: D804.exe PID: **6088**, Parent PID: **1340**

General

Target ID:	16
Start time:	10:42:41
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe --Task
Imagebase:	0x400000
File size:	802304 bytes
MD5 hash:	6944FCA258A9009F9D3B7212CDB4874D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000010.00000002.619429561.0000000000891000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000010.00000002.617846506.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000010.00000002.617846506.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000010.00000002.617846506.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000010.00000002.617846506.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	46			invalid handle	1	42E51E	WriteFile
unknown	unknown	2			invalid handle	1	42E51E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\get[1].htm	0	560	7b 22 70 75 62 6c 69 63 5f 6b 65 79 22 3a 22 2d 2d 2d 2d 2d 42 45 47 49 4e 26 23 31 36 30 3b 50 55 42 4c 49 43 26 23 31 36 30 3b 4b 45 59 2d 2d 2d 2d 2d 2d 5c 5c 6e 4d 49 49 42 49 6a 41 4e 42 67 6b 71 68 6b 69 47 39 77 30 42 41 51 45 46 41 41 4f 43 41 51 38 41 4d 49 49 42 43 67 4b 43 41 51 45 41 7a 56 56 6d 34 74 75 35 69 79 5a 77 31 33 61 5c 2f 47 69 55 30 5c 5c 6e 56 35 54 36 79 75 6d 33 6b 38 6f 58 4a 75 50 66 75 5c 2f 64 6c 44 70 35 6e 36 54 7a 6b 36 4e 38 76 6e 75 4b 70 6a 43 38 6c 6b 56 37 78 75 4d 59 67 64 74 66 51 34 63 57 59 4b 78 55 76 42 4d 61 35 5c 5c 6e 5a 6f 59 6c 7a 56 53 6c 72 49 56 65 64 51 4d 32 77 7a 32 79 4f 55 51 63 4f 49 6f 61 67 73 78 51 45 7a 76 39 4f 66 33 72 4e 79 32 67 46 34 64 72 38 32 4b 70 38 49 61 71 44 6b 30 63 33 68 6a 7a 5c	{"public_key":"-----BEGIN PUBLIC KEY-----\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzVVm4tu5iyZw13a\/GiU0\\nV5T6yum3k8oXJuPfu\/dlDp5n6Tzk6N8vnuKpjC8lkV7xuMYgdtfQ4cWYKxUvBMa5\\nZoYlzVSlrIVedQM2wz2yOUQcOloagsxQEzv9Of3rNy2gF4dr82Kp8laqDk0c3hjz\\	success or wait	1	41E975	InternetReadFile
C:\Users\user\AppData\Local\bowsakkdestx.txt	0	560	7b 22 70 75 62 6c 69 63 5f 6b 65 79 22 3a 22 2d 2d 2d 2d 2d 42 45 47 49 4e 26 23 31 36 30 3b 50 55 42 4c 49 43 26 23 31 36 30 3b 4b 45 59 2d 2d 2d 2d 2d 2d 5c 5c 6e 4d 49 49 42 49 6a 41 4e 42 67 6b 71 68 6b 69 47 39 77 30 42 41 51 45 46 41 41 4f 43 41 51 38 41 4d 49 49 42 43 67 4b 43 41 51 45 41 7a 56 56 6d 34 74 75 35 69 79 5a 77 31 33 61 5c 2f 47 69 55 30 5c 5c 6e 56 35 54 36 79 75 6d 33 6b 38 6f 58 4a 75 50 66 75 5c 2f 64 6c 44 70 35 6e 36 54 7a 6b 36 4e 38 76 6e 75 4b 70 6a 43 38 6c 6b 56 37 78 75 4d 59 67 64 74 66 51 34 63 57 59 4b 78 55 76 42 4d 61 35 5c 5c 6e 5a 6f 59 6c 7a 56 53 6c 72 49 56 65 64 51 4d 32 77 7a 32 79 4f 55 51 63 4f 49 6f 61 67 73 78 51 45 7a 76 39 4f 66 33 72 4e 79 32 67 46 34 64 72 38 32 4b 70 38 49 61 71 44 6b 30 63 33 68 6a 7a 5c	{"public_key":"-----BEGIN PUBLIC KEY-----\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzVVm4tu5iyZw13a\/GiU0\\nV5T6yum3k8oXJuPfu\/dlDp5n6Tzk6N8vnuKpjC8lkV7xuMYgdtfQ4cWYKxUvBMa5\\nZoYlzVSlrIVedQM2wz2yOUQcOloagsxQEzv9Of3rNy2gF4dr82Kp8laqDk0c3hjz\\	success or wait	1	42E51E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\SystemID\PersonalID.txt	unknown	4096	success or wait	1	42B836	ReadFile
C:\SystemID\PersonalID.txt	unknown	4096	end of file	1	42B836	ReadFile

Analysis Process: D804.exe PID: **128**, Parent PID: **772**

General

Target ID:	18
Start time:	10:42:41
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\D804.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\AppData\Local\Temp\D804.exe" --Admin IsNotAutoStart IsNotTask
Imagebase:	0x400000
File size:	802304 bytes
MD5 hash:	6944FCA258A9009F9D3B7212CDB4874D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000012.00000002.451684545.00000000024D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000012.00000002.451684545.00000000024D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000012.00000002.451349547.00000000023B3000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: D804.exe PID: **4528**, Parent PID: **128**

General

Target ID:	19
Start time:	10:42:42
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\D804.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\D804.exe" --Admin IsNotAutoStart IsNotTask
Imagebase:	0x400000
File size:	802304 bytes
MD5 hash:	6944FCA258A9009F9D3B7212CDB4874D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000013.00000002.617779609.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000013.00000002.617779609.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000013.00000002.617779609.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000013.00000002.617779609.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: 3C54.exe PID: **1720**, Parent PID: **3452**

General

Target ID:	20
Start time:	10:42:44
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\3C54.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\3C54.exe
Imagebase:	0x4a0000
File size:	5129728 bytes
MD5 hash:	2AF03D52F9CF9E53DFFC1183B403E1B7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000014.00000002.507574434.0000000004050000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_DLInjector04, Description: Detects downloader / injector, Source: C:\Users\user\AppData\Local\Temp\3C54.exe, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 70%, ReversingLabs
Reputation:	moderate

Analysis Process: aafg31.exe PID: **2336**, Parent PID: **1720**

General	
Target ID:	21
Start time:	10:42:46
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\aafg31.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\aafg31.exe"
Imagebase:	0x7ff777030000
File size:	973312 bytes
MD5 hash:	B4F79B3194235084A3EC85711EDFBD38
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 33%, ReversingLabs

Analysis Process: NewPlayer.exe PID: **4364**, Parent PID: **1720**

General	
Target ID:	22
Start time:	10:42:47
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\NewPlayer.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\NewPlayer.exe"
Imagebase:	0x60000
File size:	255488 bytes
MD5 hash:	08240E71429B32855B418A4ACF0E38EC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000016.00000000.460937652.0000000000061000.00000020.00000001.01000000.00000011.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000016.00000002.476037262.0000000000061000.00000020.00000001.01000000.00000011.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Temp\NewPlayer.exe, Author: Joe Security
Antivirus matches:	• Detection: 88%, ReversingLabs

Analysis Process: XandETC.exe PID: **5320**, Parent PID: **1720**

General	
Target ID:	23
Start time:	10:42:49
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\XandETC.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\XandETC.exe"
Imagebase:	0x7ff6a7fc0000
File size:	3890176 bytes
MD5 hash:	3006B49F3A30A80BB85074C279ACC7DF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 73%, ReversingLabs

Analysis Process: build2.exe PID: **4696**, Parent PID: **4528**

General	
Target ID:	24
Start time:	10:42:49
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe"
Imagebase:	0x400000
File size:	335360 bytes
MD5 hash:	B888EFE68F257AA2335ED9CBD63C1343
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000018.00000002.478126519.0000000000840000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000018.00000002.478487593.00000000008C8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 87%, ReversingLabs

Analysis Process: B46F.exe PID: **4928**, Parent PID: **3452**

General	
Target ID:	25
Start time:	10:42:51
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\B46F.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B46F.exe
Imagebase:	0x400000
File size:	802304 bytes
MD5 hash:	6944FCA258A9009F9D3B7212CDB4874D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000019.00000002.473949878.0000000002434000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000019.00000002.474131384.00000000024D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000019.00000002.474131384.00000000024D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: B46F.exe PID: **2576**, Parent PID: **4928**

General	
Target ID:	26
Start time:	10:42:51
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\B46F.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B46F.exe
Imagebase:	0x400000
File size:	802304 bytes
MD5 hash:	6944FCA258A9009F9D3B7212CDB4874D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000001A.00000002.488867120.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000001A.00000002.488867120.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000001A.00000002.488867120.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001A.00000002.488867120.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

Analysis Process: A170.exe PID: **1868**, Parent PID: **3452**

General

Target ID:	27
Start time:	10:42:51
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\A170.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\A170.exe
Imagebase:	0x400000
File size:	809984 bytes
MD5 hash:	15BC205C2CAF7196EE2267087C3B2BB8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000001B.00000002.493740298.00000000024C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001B.00000002.493740298.00000000024C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000001B.00000002.490286812.0000000002380000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 71%, ReversingLabs

Analysis Process: D804.exe PID: **1264**, Parent PID: **3452**

General

Target ID:	28
Start time:	10:42:52
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe" --AutoStart
Imagebase:	0x400000
File size:	802304 bytes
MD5 hash:	6944FCA258A9009F9D3B7212CDB4874D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000001C.00000002.488812684.000000000228A000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000001C.00000002.491035809.0000000002460000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001C.00000002.491035809.0000000002460000.00000040.00001000.00020000.00000000.sdmp, Author: unknown

Analysis Process: A170.exe PID: **1964**, Parent PID: **1868**

General

Target ID:	29
Start time:	10:42:53
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\A170.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\AppData\Local\Temp\A170.exe
Imagebase:	0x400000
File size:	809984 bytes
MD5 hash:	15BC205C2CAF7196EE2267087C3B2BB8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000001D.00000002.489556428.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000001D.00000002.489556428.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000001D.00000002.489556428.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001D.00000002.489556428.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

Analysis Process: build3.exe PID: **5868**, Parent PID: **4528**

General

Target ID:	30
Start time:	10:42:53
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build3.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build3.exe"
Imagebase:	0x1000000
File size:	9728 bytes
MD5 hash:	9EAD10C08E72AE41921191F8DB39BC16
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 0000001E.00000000.474017727.0000000001001000.00000020.00000001.01000000.00000016.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 0000001E.00000000.474017727.0000000001001000.00000020.00000001.01000000.00000016.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 0000001E.00000002.477600932.0000000000BDA000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 0000001E.00000002.477600932.0000000000BDA000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 0000001E.00000002.477942290.0000000001001000.00000020.00000001.01000000.00000016.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 0000001E.00000002.477942290.0000000001001000.00000020.00000001.01000000.00000016.sdmp, Author: unknown • Rule: JoeSecurity_Clipboard_Hijacker, Description: Yara detected Clipboard Hijacker, Source: C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build3.exe, Author: Joe Security • Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build3.exe, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build3.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 88%, ReversingLabs

Analysis Process: D804.exe PID: **5444**, Parent PID: **1264**

General

Target ID:	31
Start time:	10:42:53
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\de8c49a6-0e90-48ec-87c8-3cd1f6f0601e\D804.exe" --AutoStart
Imagebase:	0x400000
File size:	802304 bytes
MD5 hash:	6944FCA258A9009F9D3B7212CDB4874D
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000001F.00000002.486782772.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000001F.00000002.486782772.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000001F.00000002.486782772.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001F.00000002.486782772.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

Analysis Process: build2.exe PID: **6096**, Parent PID: **4696**

General

Target ID:	32
Start time:	10:42:53
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\0e111cbe-1163-4b86-ad03-032e194ee525\build2.exe"
Imagebase:	0x400000
File size:	335360 bytes
MD5 hash:	B888EFE68F257AA2335ED9CBD63C1343
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000020.00000002.519993720.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000020.00000002.522623167.0000000002345000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: schtasks.exe PID: **5268**, Parent PID: **5868**

General

Target ID:	33
Start time:	10:42:53
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	/C /create /F /sc minute /mo 1 /tn "Azure-Update-Task" /tr "C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe"
Imagebase:	0x12b0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 913F.exe PID: **5260**, Parent PID: **3452**

General

Target ID:	34
Start time:	10:42:53
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\913F.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\913F.exe
Imagebase:	0x400000
File size:	809984 bytes
MD5 hash:	15BC205C2CAF7196EE2267087C3B2BB8

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000022.00000002.483526399.0000000002410000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000022.00000002.483526399.0000000002410000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000022.00000002.482578416.0000000000887000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 71%, ReversingLabs

Analysis Process: mnolyk.exe PID: **5348**, Parent PID: **4364**

General

Target ID:	35
Start time:	10:42:53
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe"
Imagebase:	0xe00000
File size:	255488 bytes
MD5 hash:	08240E71429B32855B418A4ACF0E38EC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000023.00000003.612344653.0000000000C47000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000023.00000002.618034875.0000000000C47000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000023.00000002.618608332.0000000000E01000.00000020.00000001.01000000.00000018.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000023.00000000.475540855.0000000000E01000.00000020.00000001.01000000.00000018.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000023.00000003.520904242.0000000000C5E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000023.00000003.520904242.0000000000C47000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000023.00000002.618034875.0000000000C5E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000023.00000002.618034875.0000000000BE5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 88%, ReversingLabs

Analysis Process: conhost.exe PID: **5228**, Parent PID: **5268**

General

Target ID:	36
Start time:	10:42:53
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x310000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 913F.exe PID: **5512**, Parent PID: **5260**

General	
Target ID:	37
Start time:	10:42:54
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\913F.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\913F.exe
Imagebase:	0x400000
File size:	809984 bytes
MD5 hash:	15BC205C2CAF7196EE2267087C3B2BB8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000025.00000002.508274482.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000025.00000002.508274482.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000025.00000002.508274482.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000025.00000002.508274482.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

Analysis Process: F4F7.exe PID: **5436**, Parent PID: **3452**

General	
Target ID:	38
Start time:	10:42:54
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\F4F7.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\F4F7.exe
Imagebase:	0x400000
File size:	288768 bytes
MD5 hash:	7A8E3D000FBA0F5765B98E2D78EB9D12
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000026.00000002.505614178.00000000007D0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000026.00000002.505614178.00000000007D0000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000026.00000002.501652652.00000000007C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000026.00000002.508616217.0000000002231000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000026.00000002.508616217.0000000002231000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000026.00000002.506871844.00000000007F8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: mstsca.exe PID: **6600**, Parent PID: **1080**

General	
Target ID:	40
Start time:	10:42:56
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe
Imagebase:	0x9b0000

File size:	9728 bytes
MD5 hash:	9EAD10C08E72AE41921191F8DB39BC16
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 00000028.00000002.618179009.00000000009B1000.00000020.00000001.01000000.0000001A.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 00000028.00000002.618179009.00000000009B1000.00000020.00000001.01000000.0000001A.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 00000028.00000000.480111248.00000000009B1000.00000020.00000001.01000000.0000001A.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 00000028.00000000.480111248.00000000009B1000.00000020.00000001.01000000.0000001A.sdmp, Author: unknown • Rule: JoeSecurity_Clipboard_Hijacker, Description: Yara detected Clipboard Hijacker, Source: C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe, Author: Joe Security • Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe, Author: unknown
Antivirus matches:	• Detection: 88%, ReversingLabs

Analysis Process: 5DA0.exe PID: **6404**, Parent PID: **3452**

General

Target ID:	41
Start time:	10:42:57
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\5DA0.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\5DA0.exe
Imagebase:	0x9a0000
File size:	5129728 bytes
MD5 hash:	2AF03D52F9CF9E53DFFC1183B403E1B7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MALWARE_Win_DLInjector04, Description: Detects downloader / injector, Source: C:\Users\user\AppData\Local\Temp\5DA0.exe, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 70%, ReversingLabs

Disassembly

No disassembly