ID: 877000
Sample Name: 02107799.exe
Cookbook: default.jbs
Time: 10:43:07
Date: 28/05/2023
Version: 37.1.0 Beryl

Table of Contents

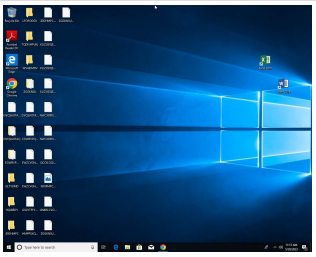
Windows Analysis Report

02107799.exe

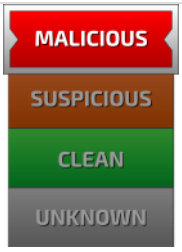
Overview

General Information

Sample Name:	02107799.exe
Analysis ID:	877000
MD5:	6017e7c6f19de..
SHA1:	605250b6daba...
SHA256:	c421418b410e...
Infos:	



Detection



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

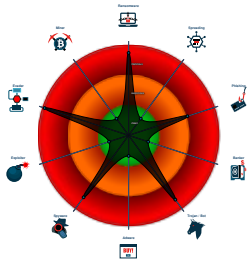
Score: 100
Range: 0 - 100

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
- Found malware configuration

Classification



Process Tree

- **System is w10x64**
- 02107799.exe (PID: 7160 cmdline: C:\Users\user\Desktop\02107799.exe MD5: 6017E7C6F19DE9E3B0AAE0965FE25603)
  - explorer.exe (PID: 3324 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - BDC0.exe (PID: 6912 cmdline: C:\Users\user\AppData\Local\Temp\BDC0.exe MD5: 6944FCA258A9009F9D3B7212CDB4874D)
      - BDC0.exe (PID: 7044 cmdline: C:\Users\user\AppData\Local\Temp\BDC0.exe MD5: 6944FCA258A9009F9D3B7212CDB4874D)
        - icacls.exe (PID: 4744 cmdline: icacls "C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8" /deny *S-1-1-0:(OI)(CI)(DE,DC) MD5: FF0D1D4317A44C951240FAE75075D501)
        - BDC0.exe (PID: 1516 cmdline: "C:\Users\user\AppData\Local\Temp\BDC0.exe" --Admin IsNotAutoStart IsNotTask MD5: 6944FCA258A9009F9D3B7212CDB4874D)
          - BDC0.exe (PID: 2900 cmdline: "C:\Users\user\AppData\Local\Temp\BDC0.exe" --Admin IsNotAutoStart IsNotTask MD5: 6944FCA258A9009F9D3B7212CDB4874D)
            - build2.exe (PID: 4724 cmdline: "C:\Users\user\AppData\Local\205aa591-8aa8-4e2c-a5b1-c9b7aaf860cf\build2.exe" MD5: B888EFE68F257AA2335ED9CBD63C1343)
    - AD22.exe (PID: 4724 cmdline: C:\Users\user\AppData\Local\Temp\AD22.exe MD5: 7A8E3D000FBA0F5765B98E2D78EB9D12)
      - WerFault.exe (PID: 3356 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4724 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - dllhost.exe (PID: 5456 cmdline: C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E} MD5: 2528137C6745C4EADD87817A1909677E)
    - 223E.exe (PID: 2952 cmdline: C:\Users\user\AppData\Local\Temp\223E.exe MD5: 2AF03D52F9CF9E53DFFC1183B403E1B7)
      - aafg31.exe (PID: 2280 cmdline: "C:\Users\user\AppData\Local\Temp\aafg31.exe" MD5: B4F79B3194235084A3EC85711EDFBD38)
      - NewPlayer.exe (PID: 2284 cmdline: "C:\Users\user\AppData\Local\Temp\NewPlayer.exe" MD5: 08240E71429B32855B418A4ACF0E38EC)
        - mnolyk.exe (PID: 6916 cmdline: "C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe" MD5: 08240E71429B32855B418A4ACF0E38EC)
          - schtasks.exe (PID: 4696 cmdline: "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN mnolyk.exe /TR "C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe" /F MD5: 15FF7D8324231381BAD48A052F85DF04)
            - conhost.exe (PID: 1280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - cmd.exe (PID: 5052 cmdline: "C:\Windows\System32\cmd.exe" /k echo Y|CACLS "mnolyk.exe" /P "user:N"&&CACLS "mnolyk.exe" /P "user:R" /E&&echo Y|CACLS "..\6d73a97b0c" /P "user:N"&&CACLS "..\6d73a97b0c" /P "user:R" /E&&Exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 4360 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - cmd.exe (PID: 1092 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Y" MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - cacls.exe (PID: 3356 cmdline: CACLS "mnolyk.exe" /P "user:N" MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
            - cacls.exe (PID: 4580 cmdline: CACLS "mnolyk.exe" /P "user:R" /E MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
            - cmd.exe (PID: 5536 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Y" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - rundll32.exe (PID: 5672 cmdline: "C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\07c6bc37dc5087\cred64.dll, Main MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
            - rundll32.exe (PID: 5812 cmdline: "C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\07c6bc37dc5087\cred64.dll, Main MD5: 73C519F050C20580F8A62C849D49215A)
      - XandETC.exe (PID: 4980 cmdline: "C:\Users\user\AppData\Local\Temp\XandETC.exe" MD5: 3006B49F3A30A80BB85074C279ACC7DF)
    - BDC0.exe (PID: 256 cmdline: "C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.exe" --AutoStart MD5:

6944FCA258A9009F9D3B7212CDB4874D)
- 946D.exe (PID: 2064 cmdline: C:\Users\user\AppData\Local\Temp\946D.exe MD5: 6944FCA258A9009F9D3B7212CDB4874D)
  - 946D.exe (PID: 4576 cmdline: C:\Users\user\AppData\Local\Temp\946D.exe MD5: 6944FCA258A9009F9D3B7212CDB4874D)
- 8DD2.exe (PID: 6048 cmdline: C:\Users\user\AppData\Local\Temp\8DD2.exe MD5: 15BC205C2CAF7196EE2267087C3B2BB8)
  - 8DD2.exe (PID: 5312 cmdline: C:\Users\user\AppData\Local\Temp\8DD2.exe MD5: 15BC205C2CAF7196EE2267087C3B2BB8)
- 794C.exe (PID: 5236 cmdline: C:\Users\user\AppData\Local\Temp\794C.exe MD5: 15BC205C2CAF7196EE2267087C3B2BB8)
  - 794C.exe (PID: 5660 cmdline: C:\Users\user\AppData\Local\Temp\794C.exe MD5: 15BC205C2CAF7196EE2267087C3B2BB8)
- DC0A.exe (PID: 4596 cmdline: C:\Users\user\AppData\Local\Temp\DC0A.exe MD5: 7A8E3D000FBA0F5765B98E2D78EB9D12)

- cuwsgii (PID: 5704 cmdline: C:\Users\user\AppData\Roaming\cuwsgii MD5: 6017E7C6F19DE9E3B0AAE0965FE25603)
- svchost.exe (PID: 3276 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 256 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 4724 -ip 4724 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - BDC0.exe (PID: 5184 cmdline: "C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.exe" --AutoStart MD5: 6944FCA258A9009F9D3B7212CDB4874D)
- BDC0.exe (PID: 4248 cmdline: C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.exe --Task MD5: 6944FCA258A9009F9D3B7212CDB4874D)
  - BDC0.exe (PID: 5484 cmdline: C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.exe --Task MD5: 6944FCA258A9009F9D3B7212CDB4874D)
- mnolyk.exe (PID: 5892 cmdline: C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe MD5: 08240E71429B32855B418A4ACF0E38EC)
- **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

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\B87Z87FM\build3[1].exe	JoeSecurity_Clipboard_Hijacker	Yara detected Clipboard Hijacker	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\build3[1].exe	Windows_Trojan_Clipbanker_f9f9e79d	unknown	unknown	• 0x1203:$a1: 7E 7E 0F B7 04 77 83 F8 41 74 69 83 F8 42 74 64 83 F8 43 74 5F 83
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\build3[1].exe	Windows_Trojan_Clipbanker_787b130b	unknown	unknown	• 0xefa:$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\Local\205aa591-8aa8-4e2c-a5b1-c9b7aaf860cf\build3.exe	JoeSecurity_Clipboard_Hijacker	Yara detected Clipboard Hijacker	Joe Security	
C:\Users\user\AppData\Local\205aa591-8aa8-4e2c-a5b1-c9b7aaf860cf\build3.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 13 entries

Memory Dumps

Source	Rule	Description	Author	Strings
00000017.00000003.507221089.0000000000877000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Amadey	Yara detected Amadey bot	Joe Security	
00000029.00000002.507218040.0000000000830000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000029.00000002.507218040.0000000000830000.00000004.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x644:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
00000007.00000002.466741568.00000000006E0000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000007.00000002.466859544.0000000000818000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x74f1:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B

Click to see the 87 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
23.0.mnolyk.exe.60000.0.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
22.0.NewPlayer.exe.ff0000.0.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	

Source	Rule	Description	Author	Strings
39.2.794C.exe.400000.0.raw.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth (Nextron Systems)	• 0xe23ea:$s1: http:// • 0x100498:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x100b28:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x100b4e:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x10472e:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x102626:$s2: \xE8\xF4\xF4\xF0\xF3\xBA\xAF\xAF • 0xe23ea:$f1: http://
39.2.794C.exe.400000.0.raw.unpack	JoeSecurity_Djvu	Yara detected Djvu Ransomware	Joe Security	
39.2.794C.exe.400000.0.raw.unpack	MALWARE_Win_STOP	Detects STOP ransomware	ditekSHen	• 0xffe88:$x1: C:\SystemID\PersonalID.txt • 0x100334:$x2: /deny *S-1-1-0:(OI)(CI)(DE,DC) • 0xffcf0:$x3: e:\doc\my work (c++)_git\encryption\ • 0x105b28:$x3: E:\Doc\My work (C++)_Git\Encryption\ • 0x1002ec:$s1: " --AutoStart • 0x100300:$s1: " --AutoStart • 0x103f48:$s2: --ForNetRes • 0x103f10:$s3: --Admin • 0x104390:$s4: %username% • 0x1044b4:$s5: ?pid= • 0x1044c0:$s6: &first=true • 0x1044d8:$s6: &first=false • 0x1003f4:$s7: delself.bat • 0x1043f8:$mutex1: {1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D} • 0x104420:$mutex2: {FBB4BCC6-05C7-4ADD-B67B-A98A697323C1} • 0x104448:$mutex3: {36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}
Click to see the 118 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

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 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)

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

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)

Sample uses process hollowing technique

Stealing of Sensitive Information

Yara detected Amadeys stealer DLL

Yara detected SmokeLoader

Yara detected Amadey bot

Yara detected Clipboard Hijacker

Yara detected Vidar stealer

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

Tries to harvest and steal ftp login credentials

Tries to steal Instant Messenger accounts or passwords

Remote Access Functionality

Yara detected SmokeLoader

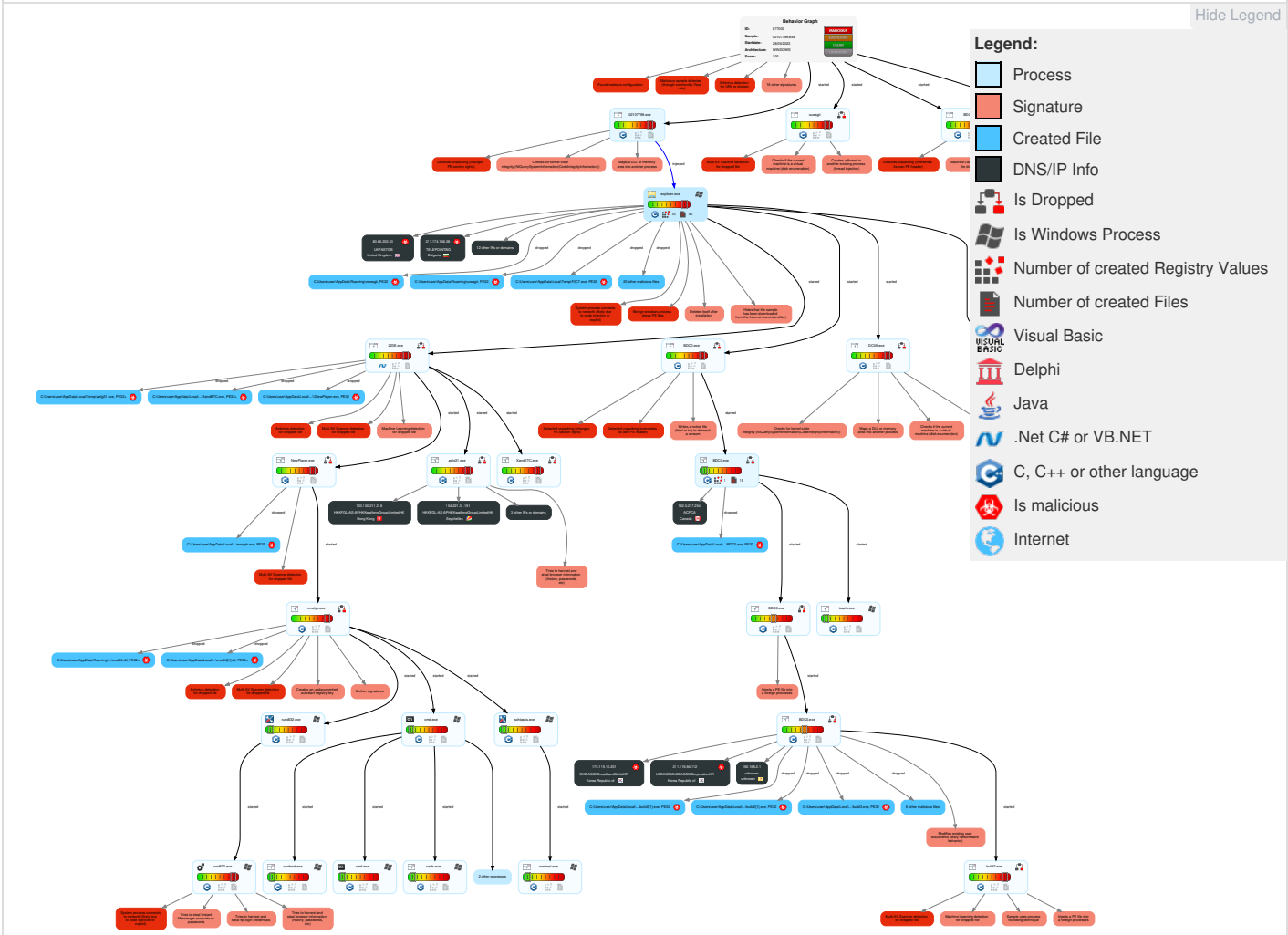
Yara detected Vidar stealer

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	5 1 2 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	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 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Shared Modules	1 Services File Permissions Weakness	1 1 Registry Run Keys / Startup Folder	3 1 Obfuscated Files or Information	1 Credentials in Registry	2 6 System Information Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Exploitation for Client Execution	Logon Script (Mac)	1 Services File Permissions Weakness	2 2 Software Packing	1 Credentials In Files	1 Query Registry	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	2 Command and Scripting Interpreter	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	4 4 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	1 Scheduled Task/Job	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	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	5 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Rundll32	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

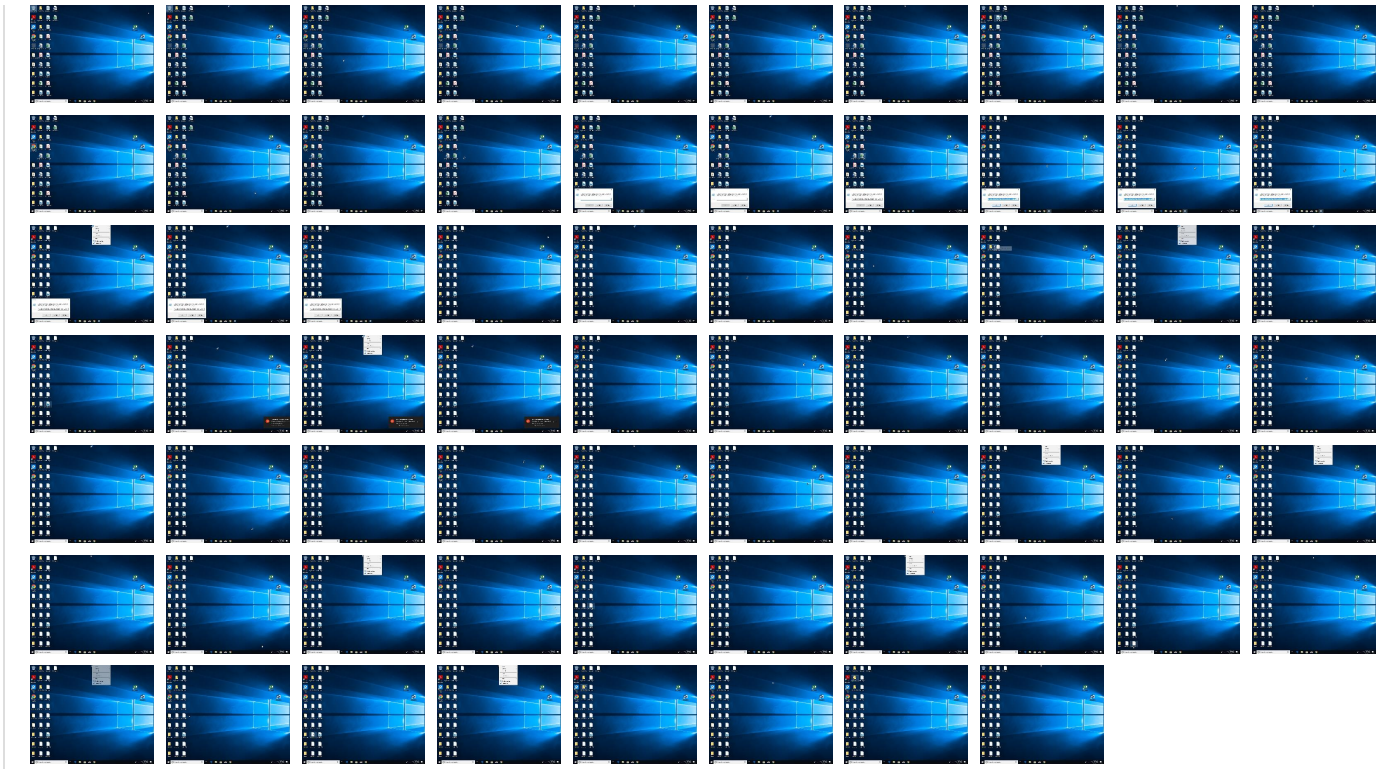
Behavior Graph



Screenshots

Thumbnails

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




Recycle Bin
LFOPODGV
JDDHMPC...
ZGGKNSU...
Acrobat Reader DC
TQDFJHPUIU
KLIZUSIQE...
Microsoft Edge
WSHEJMDV
KLIZUSIQE...
Google Chrome
ZGGKNSU
KLIZUSIQE...
EIVQSAOTA...
EIVQSAOTA...
NWCXBPIU...
EIVQSAOTAQ
EOWRVPQ...
NWCXBPIU...
EOWRVP...
EWZCVGN...
QCOILOQI...
GLTYDMD
EWZCVGN...
NYMMPC...
HQJBRDY
GIGIYTFFY...
UNKRLCVO...
JDDHMPC
HMPPSXQ...
ZGGKNSU...
Excel 2016
Word 2016
Type here to search
11:15 AM
5/28/2023

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
02107799.exe	38%	ReversingLabs		
02107799.exe	42%	Virustotal		Browse
02107799.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cred64[1].dll	100%	Avira	HEUR/AGEN.1301090	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\build3[1].exe	100%	Avira	TR/Crypt.XPACK.Gen8	
C:\Users\user\AppData\Local\Temp\223E.exe	100%	Avira	HEUR/AGEN.1357339	
C:\Users\user\AppData\Local\Temp\4445.exe	100%	Avira	HEUR/AGEN.1357339	
C:\Users\user\AppData\Local\205aa591-8aa8-4e2c-a5b1-c9b7aaf860cf\build3.exe	100%	Avira	TR/Crypt.XPACK.Gen8	
C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe	100%	Avira	HEUR/AGEN.1319380	
C:\Users\user\AppData\Local\Temp\5B59.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6A3D.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\205aa591-8aa8-4e2c-a5b1-c9b7aaf860cf\build2.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\110C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\build2[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\223E.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\4445.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\205aa591-8aa8-4e2c-a5b1-c9b7aaf860cf\build2.exe	87%	ReversingLabs	Win32.Trojan.Smokeloader	
C:\Users\user\AppData\Local\205aa591-8aa8-4e2c-a5b1-c9b7aaf860cf\build3.exe	88%	ReversingLabs	Win32.Trojan.ClipBanker	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\build2[1].exe	87%	ReversingLabs	Win32.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\build3[1].exe	88%	ReversingLabs	Win32.Trojan.ClipBanker	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cred64[1].dll	83%	ReversingLabs	Win64.Trojan.Amadey	
C:\Users\user\AppData\Local\Temp\223E.exe	70%	ReversingLabs	ByteCode-MSIL.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\4445.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\7439.exe	43%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\78BB.exe	70%	ReversingLabs	ByteCode-MSIL.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\794C.exe	71%	ReversingLabs	Win32.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\8DD2.exe	71%	ReversingLabs	Win32.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\AFA6.exe	71%	ReversingLabs	Win32.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\C45B.exe	71%	ReversingLabs	Win32.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\EB26.exe	70%	ReversingLabs	ByteCode-MSIL.Trojan.Smokeloader	
C:\Users\user\AppData\Local\Temp\F0C7.exe	71%	ReversingLabs	Win32.Trojan.Smokeloader	

Source	Detection	Scanner	Label	Link
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	
C:\Users\user\AppData\Roaming\07c6bc37dc5087\cred64.dll	83%	ReversingLabs	Win64.Trojan.Amadey	
C:\Users\user\AppData\Roaming\cuwsgii	38%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://components.groove.net/Groove/Components/SystemComponents/SystemComponents.osd?Package=net.gro	0%	URL Reputation	safe	
http://jp.imgjeoighw.com/sts/image.jpg	0%	URL Reputation	safe	
http://colisumy.com/dl/build2.exe$run	100%	URL Reputation	malware	
http://ss.apjeoighw.com/	0%	URL Reputation	safe	
http://zexeq.com/files/1/build3.exe$run	100%	URL Reputation	malware	
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://zexeq.com/raud/get.php?pid=903E7F261711F85395E5CEFBF4173C544.	100%	Avira URL Cloud	malware	
http://ss.apjeoighw.com/check/safe	0%	URL Reputation	safe	
http://colisumy.com/dl/build2.exe	100%	URL Reputation	malware	
http://ss.apjeoighw.com:80/check/?sid=437284&key=c4d583a983211d53f326aa000dca4127MjIzMSIsICJ1bl9wd2Q	0%	Avira URL Cloud	safe	
http://ss.apjeoighw.com/check/?sid=437284&key=c4d583a983211d53f326aa000dca4127	0%	Avira URL Cloud	safe	
http://zexeq.com/raud/get.phpL	100%	Avira URL Cloud	malware	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://zexeq.com/files/1/build3.exe	0%	URL Reputation	safe	
http://wuc11.com/tmp/	0%	Avira URL Cloud	safe	
http://45.9.74.80/0bjds.apjeoighw.com/	100%	Avira URL Cloud	malware	
http://ss.apjeoighw.com/check/?sid=437114&key=556b8e8f2c0037a585c40888436f6c33f	0%	Avira URL Cloud	safe	
http://ss.apjeoighw.com/check/?sid=436898&key=31b04f4e86a5030e55172a3ce21438a6f	0%	Avira URL Cloud	safe	
http://zexeq.com/raud/get.php?pid=903E7F261711F85395E5CEFBF4173C54&first=truey	100%	Avira URL Cloud	malware	
http://colisumy.com/dl/build2.exerun417	100%	Avira URL Cloud	malware	
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	0%	Avira URL Cloud	safe	
http://colisumy.com/dl/build2.exe/p	100%	Avira URL Cloud	malware	
http://ss.apjeoighw.com/check/safeS	0%	Avira URL Cloud	safe	
http://ss.apjeoighw.com/check/?sid=437232&key=35a897019d4d6b7304232007313f15f2	0%	Avira URL Cloud	safe	
45.9.74.80/0bjdn2Z/index.php	100%	Avira URL Cloud	malware	
http://zexeq.com/files/1/build3.exerun	100%	Avira URL Cloud	malware	
http://https://we.tl/t-tnzomMj6	0%	Avira URL Cloud	safe	
http://ss.apjeoighw.com/check/safe13f15f2	0%	Avira URL Cloud	safe	
http://colisumy.com/dlget.php?pid=903E7F261711F85395E5CEFBF4173C54	100%	Avira URL Cloud	malware	
http://ss.apjeoighw.com/check/?sid=437712&key=e0936dbb5215a1cc85afbf7dbb62727d	0%	Avira URL Cloud	safe	
http://ss.apjeoighw.com:80/check/?sid=436898&key=31b04f4e86a5030e55172a3ce21438a6	0%	Avira URL Cloud	safe	
http://zexeq.com/files/1/build3.exe$runyinstall020921_delay721_sec.exe0	100%	Avira URL Cloud	malware	
http://ss.apjeoighw.com:80/check/safe	0%	Avira URL Cloud	safe	
http://ss.apjeoighw.com:80/check/?sid=437058&key=7c45c7b8ba54fad24dbc26b647ebd1bc	0%	Avira URL Cloud	safe	
http://zexeq.com/files/1/build3.exe$rung	100%	Avira URL Cloud	malware	
http://ss.apjeoighw.com/check/safe1B	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://45.9.74.80/0bjds.apjeoighw.com/check/?sid=436838&key=0f2526fc923d8a6ab4c43d0a56a5696e	100%	Avira URL Cloud	malware	
http://ss.apjeoighw.com:80/check/?sid=437114&key=556b8e8f2c0037a585c40888436f6c335	0%	Avira URL Cloud	safe	
http://zexeq.com/files/1/build3.exe$runP	100%	Avira URL Cloud	malware	
http://zexeq.com/raud/get.phpep	100%	Avira URL Cloud	malware	
http://ss.apjeoighw.com:80/check/safeD	0%	Avira URL Cloud	safe	
http://https://we.tl/t-tnzomMj6$	0%	Avira URL Cloud	safe	
http://ladogatur.ru/tmp/	0%	Avira URL Cloud	safe	
http://ss.apjeoighw.com/check/?sid=437058&key=7c45c7b8ba54fad24dbc26b647ebd1bcf	0%	Avira URL Cloud	safe	
http://toobussy.com/tmp/	100%	Avira URL Cloud	malware	
http://https://we.tl/t-tnzomMj6HU	0%	Avira URL Cloud	safe	
http://zexeq.com/raud/get.php?pid=903E7F261711F85395E5CEFBF4173C54&first=trueb	100%	Avira URL Cloud	malware	
http://zexeq.com/raud/get.php?pid=903E7F261711F85395E5CEFBF4173C54	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://t.me/looking_glassbot	false		high
http://wuc11.com/tmp/	true	• Avira URL Cloud: safe	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://kingpirate.ru/tmp/	true	• URL Reputation: safe	unknown
http://toobussy.com/tmp/	true	• Avira URL Cloud: malware	unknown
http://ladogatur.ru/tmp/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.9.74.80/0bjds.apjeoighw.com/	aafg31.exe, 00000015.00000003.747091320.0000020955D07000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.785925314.0000020955D0E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.872189879.00020955D0E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.802910134.0000020955D0E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.847680947.0000020955D0E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.747762577.0000020955D10000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.679386130.0000020953C59000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.839605379.0000020955D12000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.764921022.0000020955D12000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://zexeq.com/raud/get.php?pid=903E7F261711F85395E5CEFBF4173C544.	BDC0.exe, 00000011.00000002.897516846.000000005B4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/yn/r/A-4As8UDAZ8.js?_nc_x=lj3Wp8lg5Kz	aafg31.exe, 00000015.00000003.871483645.0000020955D5B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661860603.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682406444.00000020955D44000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682234652.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610458087.0000020955D0D000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D14000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.725252342.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727653565.0000020955D47000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.726734363.0000020955D43000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.748027526.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.608542388.0000020955D2B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.869877378.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.609917388.00000020955D07000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.587487365.0000020955D3F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D95000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.891215691.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610990462.0000020955D0F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.892118052.0000020955D54000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D4A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727362332.0000020955D46000.00000004.00000020.00020000.00000000.sdmp	false		high
http://zexeq.com/raud/get.phpL	BDC0.exe, 00000011.00000002.897516846.0000000000613000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ss.apjeoighw.com/check/?sid=437284&key=c4d583a983211d53f326aa000dca4127	aafg31.exe, 00000015.00000003.785925314.0000020955D0E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.802910134.0000020955D0E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.847680947.00000020955D0E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.839605379.0000020955D12000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.764921022.0000020955D12000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/y-/l/0	aafg31.exe, 00000015.00000003.727362332.0000020955D46000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661661754.0000020955D07000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://static.xx.fbcdn.net/rsrc.php/v3/y4/r/ZZnKfYusN8Z.js?_nc_x=Ij3Wp8lg5Kz	aafg31.exe, 00000015.00000003.871483645.0000020955D5B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661860603.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682406444.00000020955D44000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682234652.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610458087.0000020955D0D000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D14000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.725252342.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727653565.0000020955D47000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.726734363.0000020955D43000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.748027526.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.608542388.0000020955D2B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.869877378.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.609917388.00000020955D07000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.587487365.0000020955D3F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D95000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.891215691.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610990462.0000020955D0F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.892118052.0000020955D54000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D4A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727362332.0000020955D46000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://static.xx.fbcdn.net/rsrc.php/v3/yt/r/v75M7CPu9-P.js?_nc_x=lj3Wp8lg5Kz	aafg31.exe, 00000015.00000003.871483645.0000020955D5B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661860603.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682406444.00000020955D44000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682234652.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610458087.0000020955D0D000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D14000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.725252342.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727653565.0000020955D47000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.726734363.0000020955D43000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.748027526.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.608542388.0000020955D2B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.869877378.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.609917388.00000020955D07000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.587487365.0000020955D3F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D95000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.891215691.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610990462.0000020955D0F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.892118052.0000020955D54000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D4A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727362332.0000020955D46000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ss.apjeoighw.com:80/check/?sid=437284&key=c4d583a983211d53f326aa000dca4127MjIzMSIsICJ1bl9wd2Q	aafg31.exe, 00000015.00000003.765330499.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.775551486.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.853929000.00000020953C14000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.789517605.0000020953C1A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.767549181.0000020953C1A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.803618288.0000020953C1A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.853735463.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://messenger.com/	aafg31.exe, 00000015.00000003.871483645.0000020955D5B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661860603.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682406444.00000020955D44000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682234652.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.891564020.0000020955D76000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.725526339.0000020955D63000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610458087.0000020955D0D000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D14000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.725252342.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727653565.0000020955D47000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.726734363.0000020955D43000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.748027526.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.608542388.00000020955D2B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.869877378.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.609917388.0000020955D07000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.587487365.0000020955D3F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D95000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.891215691.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610990462.0000020955D0F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.892118052.0000020955D54000.00000004.00000020.00020000.00000000.sdmp	false		high
http://components.groove.net/Groove/Components/SystemComponents/SystemComponents.osd?Package=net.gro	explorer.exe, 00000001.00000000.396414870.00007FFA13109000.00000002.00000001.01000000.00000005.sdmp	false	• URL Reputation: safe	unknown
http://jp.imgjeoighw.com/sts/image.jpg	aafg31.exe, 00000015.00000003.518091220.0000020953BEF000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.527562190.0000020953BEF000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.493686172.00000020953BEF000.00000004.00001000.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.511244929.0000020953BEF000.00000004.00000001.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.895672737.0000020953BC3000.00000004.00000001.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.502518645.0000020953BEF000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/yL/r/camCPYrr6r7.js?_nc_x=Ij3Wp8lg5Kz	aafg31.exe, 00000015.00000003.871483645.0000020955D5B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661860603.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682406444.00000020955D44000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.872402384.0000020953C62000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682234652.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610458087.0000020955D0D000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.585095031.0000020953C04000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.872402384.0000020953C16000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682568528.0000020955D10000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.872189879.0000020955D0E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.892118052.0000020955D48000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D14000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.725252342.00020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727653565.0000020955D47000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.747896229.0000020955CFE000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.871983191.0000020955D48000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.726734363.0000020955D43000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.748027526.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.608542388.0000020955D2B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.869877378.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.609917388.0000020955D07000.00000004.00000020.00020000.00000000.sdmp	false		high
http://colisumy.com/dl/build2.exe$run	BDC0.exe, 00000013.00000002.912417927.000000008ED000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://ss.apjeoighw.com/	aafg31.exe, 00000015.00000003.702328602.0000020955D15000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.963156667.0000020955A80000.00000040.00001000.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.928321825.00020955550000.00000004.00001000.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.898715266.0000020953C70000.00000040.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ss.apjeoighw.com/check/?sid=437114&key=556b8e8f2c0037a585c40888436f6c33f	aafg31.exe, 00000015.00000003.685325297.0000020953C59000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.amazon.com/	BDC0.exe, 00000013.00000003.476305321.000000009890000.00000004.00001000.00020000.00000000.sdmp	false		high
http://ss.apjeoighw.com/check/?sid=436898&key=31b04f4e86a5030e55172a3ce21438a6f	aafg31.exe, 00000015.00000003.613408935.0000020953C59000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://zexeq.com/files/1/build3.exe$run	BDC0.exe, 00000013.00000002.912417927.000000008ED000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://www.twitter.com/	BDC0.exe, 00000013.00000003.476625971.000000009890000.00000004.00001000.00020000.00000000.sdmp	false		high
http://zexeq.com/raud/get.php?pid=903E7F261711F85395E5CEFBF4173C54&first=truey	BDC0.exe, 00000013.00000002.912417927.000000008F8000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://colisumy.com/dl/build2.exerun417	BDC0.exe, 00000013.00000002.912417927.000000008ED000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://colisumy.com/dl/build2.exe/p	BDC0.exe, 00000013.00000002.912417927.000000000868000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.openssl.org/support/faq.html	BDC0.exe, 00000013.00000002.895386251.000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://ss.apjeoighw.com/check/?sid=437232&key=35a897019d4d6b7304232007313f15f2	aafg31.exe, 00000015.00000003.747091320.0000020955D07000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.785925314.0000020955D0E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.802910134.0000020955D0E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.847680947.0000020955D0E000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.747762577.0000020955D10000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.839605379.0000020955D12000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.764921022.0000020955D12000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ss.apjeoighw.com/check/safeS	aafg31.exe, 00000015.00000003.753128296.0000020953C01000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.748891799.0000020953C04000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	BDC0.exe, 00000005.00000002.453783695.000000002510000.00000040.00001000.00020000.00000000.sdmp, BDC0.exe, 00000006.00000002.461344715.0000000000400000.00000040.00000400.00020000.00000000.sdmp, BDC0.exe, 0000000B.00000002.463587041.00000000002480000.00000040.00001000.00020000.00000000.sdmp, BDC0.exe, 00000011.00000002.895547083.0000000000400000.00000040.00000400.00020000.00000000.sdmp, BDC0.exe, 00000012.00000002.463532414.0000000002410000.00000040.00001000.00020000.00000000.sdmp, BDC0.exe, 00000013.00000002.895386251.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/yT/r/Kp9IMjEGN_T.js?_nc_x=Ij3Wp8lg5Kz	aafg31.exe, 00000015.00000003.871483645.0000020955D5B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661860603.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682406444.00000020955D44000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682234652.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610458087.0000020955D0D000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D14000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.725252342.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727653565.0000020955D47000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.726734363.0000020955D43000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.748027526.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.608542388.0000020955D2B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.869877378.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.609917388.00000020955D07000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.587487365.0000020955D3F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D95000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.891215691.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610990462.0000020955D0F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.892118052.0000020955D54000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D4A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727362332.0000020955D46000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.jsonFA	BDC0.exe, 00000013.00000003.464201683.000000008AD000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/yE/r/yWg6mkUCjYR.js?_nc_x=Ij3Wp8lg5Kz	aafg31.exe, 00000015.00000003.871483645.0000020955D5B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661860603.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682406444.00000020955D44000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682234652.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610458087.0000020955D0D000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D14000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.725252342.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727653565.0000020955D47000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.726734363.0000020955D43000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.748027526.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.608542388.0000020955D2B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.869877378.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.609917388.00020955D07000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.587487365.0000020955D3F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.00000020955D95000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.891215691.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610990462.0000020955D0F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.892118052.0000020955D54000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D4A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727362332.0000020955D46000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.jsonz	BDC0.exe, 00000013.00000003.464201683.000000008AD000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000013.00000002.912417927.0000000000868000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.jsonr	BDC0.exe, 00000013.00000003.464201683.000000008AD000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000013.00000002.912417927.0000000000868000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net	aafg31.exe, 00000015.00000003.589214326.0000020953C64000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.586782794.0000020953C64000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://we.tl/t-tnzomMj6	BDC0.exe, 00000011.00000002.897516846.000000000613000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000013.00000002.912417927.0000000000907000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://zexeq.com/files/1/build3.exerun	BDC0.exe, 00000013.00000002.912417927.000000008ED000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000013.00000002.937078432.00000000031F7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://ss.apjeoighw.com/check/safe13f15f2	aafg31.exe, 00000015.00000003.748891799.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	BDC0.exe, 00000013.00000003.476541733.000000009890000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/yq/l/0	aafg31.exe, 00000015.00000003.727362332.0000020955D46000.00000004.00000020.00020000.00000000.sdmp	false		high
http://colisumy.com/dlget.php?pid=903E7F261711F85395E5CEFBF4173C54	BDC0.exe, 00000011.00000002.897516846.000000000568000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://zexeq.com/files/1/build3.exe$runyinstall020921_delay721_sec.exe0	BDC0.exe, 00000013.00000002.912417927.000000000868000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000001.00000000.38290977.000000000091F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.nytimes.com/	BDC0.exe, 00000013.00000003.476513071.000000009890000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.jsonX	BDC0.exe, 00000006.00000002.461754674.000000000622000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yE/l/0	aafg31.exe, 00000015.00000003.727362332.0000020955D46000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661661754.0000020955D07000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/	BDC0.exe, 00000013.00000003.464201683.000000008AD000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000013.00000002.912417927.000000000868000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/y2/l/0	aafg31.exe, 00000015.00000003.871483645.0000020955D5B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661860603.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682406444.000020955D44000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682234652.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610458087.0000020955D0D000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D14000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.725252342.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727653565.0000020955D47000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.726734363.0000020955D43000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.748027526.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.608542388.0000020955D2B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.869877378.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.609917388.000020955D07000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.587487365.0000020955D3F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D95000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.891215691.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610990462.0000020955D0F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.892118052.0000020955D54000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D4A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727362332.0000020955D46000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ss.apjeoighw.com/check/?sid=437712&key=e0936dbb5215a1cc85afbf7dbb62727d	aafg31.exe, 00000015.00000002.972077905.0000020955BFD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/yP/l/0	aafg31.exe, 00000015.00000003.727362332.0000020955D46000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661661754.0000020955D07000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ss.apjeoighw.com:80/check/?sid=436898&key=31b04f4e86a5030e55172a3ce21438a6	aafg31.exe, 00000015.00000003.644636498.0000020953C1A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.633428878.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.626742491.00020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.640779902.0000020953C1A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.653577716.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.635219550.0000020953C1A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.615362679.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.613408935.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.648067767.0000020953C1A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.639945801.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://components.groove.net/Groove/Components/Root.osd?Package=net.groove.Groove.Tools.System.Groov	explorer.exe, 00000001.00000000.39641487 0.00007FFA13109000.00000002.00000001.01000000.00000005.sdmp	false	• URL Reputation: safe	unknown
http://ss.apjeoighw.com/check/safe	aafg31.exe, 00000015.00000003.589214326.0000020953C04000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.928321825.0000020955550000.00000004.00001000.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.895672737.00020953B7B000.00000004.00000001.00020000.00000000.sdmp, aafg31.exe, 00000015.00000002.898715266.0000020953C70000.00000040.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://colisumy.com/dl/build2.exe	BDC0.exe, 00000013.00000002.912417927.00000000868000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000013.00000002.912417927.00000000008ED000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ss.apjeoighw.com:80/check/safe	aafg31.exe, 00000015.00000003.644636498.0000020953C1A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.718720439.0000020953C1A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.633428878.00000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.708902609.0000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.626742491.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.640779902.0000020953C1A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.703897096.0000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.653577716.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.686001799.0000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.697812636.0000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.678658664.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.703042210.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.685325297.00000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.691479412.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.708488932.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.718518496.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.635219550.0000020953C1A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.679386130.0000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.684916045.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.615362679.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.613408935.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.2ip.ua/geo.json;?	BDC0.exe, 00000011.00000002.897516846.000000005B4000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000011.00000003.466616880.00000000005B3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yO/r/_tJ17sGyxOX.js?_nc_x=lj3Wp8lg5Kz	aafg31.exe, 00000015.00000002.896936074.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610052648.0000020953C62000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.747458130.00000020953C62000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.748891799.0000020953C62000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727495452.0000020953C63000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610737115.0000020953C62000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.2ip.ua/geo.json	BDC0.exe, 00000005.00000002.453783695.00000000002510000.00000040.00001000.00020000.00000000.sdmp, BDC0.exe, 00000006.00000002.461344715.0000000000400000.00000040.00000400.00020000.00000000.sdmp, BDC0.exe, 00000006.00000002.461754674.0000000000622000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 0000000B.00000002.463587041.0000000002480000.00000040.00001000.00020000.00000000.sdmp, BDC0.exe, 00000011.00000002.897516846.00000000005B4000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000011.00000002.895547083.0000000000400000.00000040.00000400.00020000.00000000.sdmp, BDC0.exe, 00000011.00000002.897516846.0000000000568000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000011.00000003.466616880.00000000005B3000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000012.00000002.463532414.0000000002410000.00000040.00001000.00020000.00000000.sdmp, BDC0.exe, 00000013.00000003.464201683.00000000008AD000.00000004.00020.00020000.00000000.sdmp, BDC0.exe, 00000013.00000002.895386251.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://ss.apjeoighw.com:80/check/?sid=437058&key=7c45c7b8ba54fad24dbc26b647ebd1bc	aafg31.exe, 00000015.00000003.678658664.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.679386130.0000020953C18000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://zexeq.com/files/1/build3.exe$rung	BDC0.exe, 00000013.00000002.912417927.000000008ED000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ss.apjeoighw.com:80/check/?sid=437114&key=556b8e8f2c0037a585c40888436f6c335	aafg31.exe, 00000015.00000003.718720439.0000020953C1A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.708902609.0000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.703897096.0000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.686001799.0000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.725776709.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.697812636.0000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.703042210.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.685325297.0000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.691479412.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.708488932.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.718518496.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.684916045.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727495452.0000020953C18000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ss.apjeoighw.com/check/safe1B	aafg31.exe, 00000015.00000002.972077905.0000020955BFD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.9.74.80/0bjds.apjeoighw.com/check/?sid=436838&key=0f2526fc923d8a6ab4c43d0a56a5696e	aafg31.exe, 00000015.00000003.589214326.0000020953C59000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://api.2ip.ua/geo.json#?	BDC0.exe, 00000011.00000002.897516846.00000000005B4000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000011.00000003.466616880.00000000005B3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://zexeq.com/files/1/build3.exe$runP	BDC0.exe, 00000013.00000002.912417927.000000008ED000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://zexeq.com/raud/get.phpep	BDC0.exe, 00000011.00000002.897516846.00000000613000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000013.00000002.912417927.0000000000907000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ss.apjeoighw.com:80/check/safeD	aafg31.exe, 00000015.00000003.718720439.0000020953C1A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.708902609.0000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.703897096.00020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.686001799.0000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.725776709.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.697812636.0000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.703042210.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.685325297.0000020953C18000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.691479412.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.708488932.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.718518496.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.684916045.0000020953C0C000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727495452.00020953C18000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/	BDC0.exe, 00000013.00000003.476682552.00000000989000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/H	BDC0.exe, 00000013.00000003.464201683.000000008AD000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000013.00000002.912417927.0000000000868000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://we.tl/t-tnzomMj6$	BDC0.exe, 00000011.00000002.897516846.00000000613000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ss.apjeoighw.com/check/?sid=437058&key=7c45c7b8ba54fad24dbc26b647ebd1bcf	aafg31.exe, 00000015.00000003.679386130.0000020953C59000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

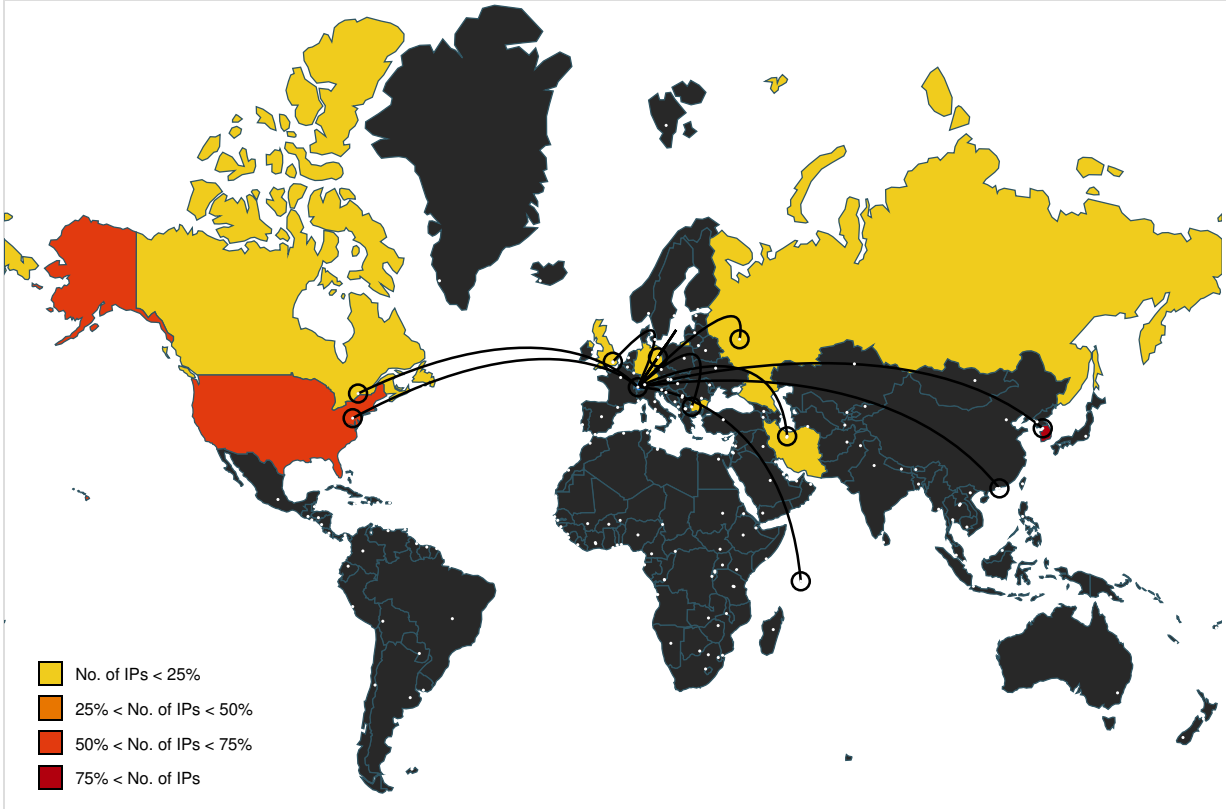
Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://static.xx.fbcdn.net/rsrc.php/v3/ye/r/sczXDyPA0UL.js?_nc_x=lj3Wp8lg5Kz	aafg31.exe, 00000015.00000003.871483645.0000020955D5B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661860603.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682406444.00000020955D44000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682234652.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610458087.0000020955D0D000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D14000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.725252342.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727653565.0000020955D47000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.726734363.0000020955D43000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.748027526.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.608542388.0000020955D2B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.869877378.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.609917388.00000020955D07000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.587487365.0000020955D3F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D95000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.891215691.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610990462.0000020955D0F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.892118052.0000020955D54000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D4A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727362332.0000020955D46000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.wikipedia.com/	BDC0.exe, 00000013.00000003.476659640.00000000009890000.00000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://we.tl/t-tnzomMj6HU	BDC0.exe, 00000011.00000002.897516846.00000000006130000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000011.00000002.897516846.0000000000632000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000013.00000002.912417927.00000000009070000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://zexeq.com/raud/get.php?pid=903E7F261711F85395E5CEFBF4173C54&first=trueb	BDC0.exe, 00000013.00000002.912417927.000000008F8000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.xx.fbcdn.net/rsrc.php/v3/yB/l/0	aafg31.exe, 00000015.00000003.871483645.0000020955D5B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661860603.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682406444.0000020955D44000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682234652.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610458087.0000020955D0D000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D14000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.725252342.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727653565.0000020955D47000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.726734363.0000020955D43000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.748027526.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.608542388.0000020955D2B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.869877378.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.609917388.0000020955D07000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.587487365.0000020955D3F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D95000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.891215691.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610990462.0000020955D0F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.892118052.0000020955D54000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D4A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727362332.0000020955D46000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://static.xx.fbcdn.net/rsrc.php/v3i7M54/yx/l/en_US/LsRZeEzcd6B.js?_nc_x=Ij3Wp8lg5Kz	aafg31.exe, 00000015.00000003.871483645.0000020955D5B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661860603.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682406444.00000020955D44000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.682234652.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610458087.0000020955D0D000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D14000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.725252342.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727653565.0000020955D47000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.726734363.0000020955D43000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.748027526.0000020955D9B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.608542388.0000020955D2B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.869877378.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.609917388.00000020955D07000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.661265412.0000020955D4B000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.587487365.0000020955D3F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D95000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.891215691.0000020955C11000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.610990462.0000020955D0F000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.892118052.0000020955D54000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.746443120.0000020955D4A000.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.727362332.0000020955D46000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.live.com/	BDC0.exe, 00000013.00000003.476481044.00000000989000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/:m	BDC0.exe, 00000006.00000002.461754674.00000000653000.00000004.00000020.00020000.00000000.sdmp	false		high
http://zexeq.com/files/1/build3.exe	BDC0.exe, 00000013.00000002.937078432.000000031EB000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000013.00000002.912417927.0000000000907000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000013.00000002.912417927.00000000008ED000.00000004.00000020.00020000.00000000.sdmp, BDC0.exe, 00000013.00000002.937078432.00000000031F7000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://static.xx.fbcdn.net/rsrc.php/v3/yI/r/Ib90vcVxYzI.js?_nc_x=Ij3Wp8lg5Kz	aafg31.exe, 00000015.00000003.661727127. 0000020953C60000.00000004.00000020.00020 000.00000000.sdmp, aafg31.exe, 00000015. 00000002.896936074.0000020953C0C000.0000 0004.00000020.00020000.00000000.sdmp, aa fg31.exe, 00000015.00000003.610052648.00 00020953C62000.00000004.00000020.0002000 0.00000000.sdmp, aafg31.exe, 00000015.00 000003.747458130.0000020953C62000.000000 04.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.678658664.0000020953C630 00.00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.748891799.00000 20953C62000.00000004.00000020.00020000.0 0000000.sdmp, aafg31.exe, 00000015.00000 003.727495452.0000020953C63000.00000004. 00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.586782794.0000020953C64000. 00000004.00000020.00020000.00000000.sdmp, aafg31.exe, 00000015.00000003.61073711 5.0000020953C62000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://zexeq.com/raud/get.php?pid=903E7F261711F85395E5CEFBF4173C54	BDC0.exe, 00000011.00000002.897516846.00 000000005B4000.00000004.00000020.0002000 0.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.google.com/	BDC0.exe, 00000013.00000003.476398741.00 00000009890000.00000004.00001000.0002000 0.00000000.sdmp	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yK/l/0	aafg31.exe, 00000015.00000003.727362332. 0000020955D46000.00000004.00000020.00020 000.00000000.sdmp, aafg31.exe, 00000015. 00000003.661661754.0000020955D07000.0000 0004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.240.9.35	unknown	United States		32934	FACEBOOKUS	false
103.100.211.218	unknown	Hong Kong		133115	HKKFGL-AS-APHKKwaifongGroupLimitedHK	false
154.221.31.191	unknown	Seychelles		133115	HKKFGL-AS-APHKKwaifongGroupLimitedHK	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.240.17.35	unknown	United States		32934	FACEBOOKUS	false
217.174.148.28	unknown	Bulgaria		31083	TELEPOINTBG	true
175.119.10.231	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
8.8.8.8	unknown	United States		15169	GOOGLEUS	false
211.40.39.251	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
157.240.17.17	unknown	United States		32934	FACEBOOKUS	false
211.171.233.129	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
211.119.84.112	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
162.0.217.254	unknown	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	unknown	United Kingdom		61323	UKFASTGB	true
45.9.74.80	unknown	Russian Federation		200740	FIRST-SERVER-EU-ASRU	true
211.59.14.90	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
20.189.173.21	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
188.114.97.7	unknown	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
80.210.25.252	unknown	Iran (ISLAMIC Republic Of)		12880	DCI-ASIR	true
222.236.49.123	unknown	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:	877000
Start date and time:	2023-05-28 10:43:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 14s
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:	50
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:	02107799.exe
Detection:	MAL

Classification:	mal100.rans.phis.troj.spyw.evad.winEXE@105/269@0/25
EGA Information:	Failed
HDC Information:	• Successful, ratio: 40.5% (good quality ratio 34.6%) • Quality average: 62.2% • 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 • Override analysis time to 240s for rundll32

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- Created / dropped Files have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, Conhost.exe, dllhost.exe, consent.exe, conhost.exe, svchost.exe
- 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 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 NtEnumerateKey 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 NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Skipping network analysis since amount of network traffic is too extensive

Simulations

Behavior and APIs

Time	Type	Description
10:44:29	API Interceptor	1552x Sleep call for process: explorer.exe modified
10:44:30	Task Scheduler	Run new task: Firefox Default Browser Agent 8DB0A56B8EC45137 path: C:\Users\user\AppData\Roaming\cuwsgii
10:44:37	Task Scheduler	Run new task: Time Trigger Task path: C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.exe s>--Task
10:44:38	API Interceptor	1x Sleep call for process: dllhost.exe modified
10:44:38	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.exe" --AutoStart
10:44:41	API Interceptor	1x Sleep call for process: WerFault.exe modified
10:44:43	API Interceptor	1x Sleep call for process: BDC0.exe modified
10:44:47	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.exe" --AutoStart
10:44:48	API Interceptor	1827x Sleep call for process: mnolyk.exe modified
10:44:53	Task Scheduler	Run new task: mnolyk.exe path: C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe
10:44:59	Task Scheduler	Run new task: Azure-Update-Task path: C:\Users\user\AppData\Roaming\Microsoft\Network\mstsca.exe
10:45:20	Task Scheduler	Run new task: Firefox Default Browser Agent 77EB2ECBEC3BD541 path: C:\Users\user\AppData\Roaming\vwwsgii
10:45:49	API Interceptor	3x Sleep call for process: aafg31.exe modified
10:45:56	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\Microsoft\Windows\WER\ReportQueue\AppCrash_AD22.exe_bc3690d31fe876d95d6ec65d5dc56974b7b47db_5f8597d0_0d70ed7f\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):	0.8200346039459757
Encrypted:	false
SSDEEP:	96:ebo1FE6KZIo+4Eyyo9Cto07RP6tpXIQcQjc6ieAcElcw3kvz+HbHg/8BRTf3o8FI:X+x3DvHtGZvPjIg/u7sBS274ltf8
MD5:	21837DE30B9C41BCF5572CF4984E6C4D
SHA1:	4B9B7534939C5FF21C2BB5B31F62CB679039754D
SHA-256:	A7B579230F92DEF3571B761BA0B55551D189E10126077487128F943F0F69F920
SHA-512:	AF176DB9A5240D9FBD1CF35BAB0DE7A0A7B4DED30B32B49E45B03BC0EC36F8C1D5DCAC99D83A8E7E1710F3EFF2BABE78272AD3AD6BF0BEBBC6B6F252C67C3EFA
Malicious:	false
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.=.1.3.3.2.9.7.6.9.4.7.7.7.8.8.0.0.2.7.....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.=.1.3.3.2.9.7.6.9.4.7.8.7.4.1.1.1.2.1.....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.=.5.5.d.6.b.1.c.2.-.2.b.2.a.-.4.7.0.5.-.b.c.3.b.-.6.c.2.2.f.9.7.4.1.f.f.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.=.c.d.b.c.6.5.4.e.-.8.9.5.a.-.4.1.6.5.-.a.c.0.f.-.b.4.b.e.b.9.1.0.e.e.5.e.....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.=.A.D.2.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.2.7.4.-.0.0.0.1.-.0.0.1.9.-.2.6.3.f.-.d.f.1.1.8.c.9.1.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.2.1.0.1.e.4.1.3.4.2.6.1.6.e.a.b.e.5.e.3.a.1.9.2.f.9.9.5.2.a.5.c.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.!.A.D.2.2...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\WER192B.tmp.csv

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	84502
Entropy (8bit):	3.0502356873357246
Encrypted:	false
SSDEEP:	768:IMHf3EX994+iZmlPnXMlnGacOnuXvrZEiOS2fkRQzN:IMHfE949mlMGaJuXTZEiOSDReN
MD5:	9054E137D33482218DED22C21F21E3AB
SHA1:	5E023D86972727F14614534AF8484CD63963CB3F
SHA-256:	B0F06D73C08A1F0EAC02B5F95C9C0001B6CEB2AF60F7CC77DFF51FD7C7B1DFB1
SHA-512:	7384CC6BAF5FFA7B3B79BA02F8660E99A537567A9C44520A46716F04F94D012539B441160B78B266524B8A84F0082DEC0A39032240C1226BA4744B4771FD30BA
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BEB.tmp.csv

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	84914
Entropy (8bit):	3.0495475191353876

Encrypted:	false
SSDEEP:	768:koHZUEig9V+iZmlPEMl+G/XOxufzrZEiOg1NC3WtOp:koHZL9V9mlcG/GufnZEiOg63Wsp
MD5:	C0B23B19EBE767440107430D2E40973C
SHA1:	86F3F877CF8DDB856BA80A1EF06AE79AE1EE0054
SHA-256:	1357D57BD2B69EF485C5DB8A5A37258F8D4F36DD0D8CFB0F47C059C3F522D295
SHA-512:	2685CB784548CA468210E32EB3A82372F0C93754A206A98213FD6E0FE7683E3A59E3C8DC103809BAFC6B423667CC20457F00863C181A9C8E00412D5062506029
Malicious:	false
Preview:	l.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2429.tmp.txt

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.699477919625044
Encrypted:	false
SSDEEP:	96:kiZYWIM3c5cDuXYhYJWhz5HSYYEZpot8i05v4PwXHtar8HpjaLkIzJ3:hZD9ymFd9Nar8HpjaLTzJ3
MD5:	1CC544F03DA59CDF8B6EF4B8DB16F1B9
SHA1:	0EFBD3FED119F86B3A0C26609F1EC6E6D2BC13D7
SHA-256:	AB5CB5A2FDDD5E01F2369FE3626ED11D17BF87154019A5A27FD0C73A4D0F6AEC
SHA-512:	BA33E878813AC9C244C56F6B64B99FD6CBBA97C496C32E2FE268C3B6CD23352EFA7CA577F5B0E93473D4687E6A18EE9F7C7ECDF075DED80B44F0B8691FD07(29
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.2.6.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2861.tmp.txt

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6997324121640456
Encrypted:	false
SSDEEP:	96:kiZYWVyR48SDoYZYVWG/EH7YEZVnt8io5v4jwweKa78HD6aToI1J3:hZDU+RnFa78HD6aTP1J3
MD5:	0E70EAC71FB36CE04D69E9D26CFDAC31
SHA1:	F29F0753323A22F32007861C9EFE1251287E94AC
SHA-256:	578E947C44FBE7184017E3DA5A1ACADC0008FF9C416944709FAE16491EABD21B
SHA-512:	4F28102AD94314A2F960B0A692B785580248EBB8FAF0F203B23A4121B89142C6866B2E7EE323CDC0C6308B670919E1E26D15CE2728A7CE51D082976A15B972CE
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.2.6.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WER338D.tmp.csv

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	85000
Entropy (8bit):	3.049733465029089
Encrypted:	false
SSDEEP:	768:irHe2EfNsO25iZmlPrbxGSvOybdurZEiO3aJZ0PlDf:irHe7sBcmlD1GS1bdUZEiOqZOlDf
MD5:	5F72A06B57F8EB5A2105CECE15D88A79

SHA1:	F6F5942ABAA2DB9FB81C8596374122846FF08D2B
SHA-256:	721D5DDB67937B7723CE112D887F75124769BEFAFE84C630E3D11A493E83C081
SHA-512:	D22DA708C3F58D42059FCE5AEBA50C49E7BA6EBE87D2ACF43053A05894333A9CE55CF628963ECF6613A3F60D3D1FE6AEF76713F0DCBEFAF06EEA7436007525 04
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H. i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,. P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a. g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a. t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T. r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3747.tmp.txt

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6998437696815176
Encrypted:	false
SSDEEP:	96:kiZYWwlJJk6YKYLWkfHEYEZPtt8iK5B4fwZOpha68H1/U8sltI5RJ3:hZDwR93g0ha68H1vsly/J3
MD5:	E91D85B6461AFF9C14FD27D9ABA8EE8A
SHA1:	1679B1985D996E97385C1E8A0C5C2CB4AF9CA677
SHA-256:	B80B376AE32F2CD618C74094A9A7CB012A440DE6BB1D53978044DB2E0CB06C24
SHA-512:	D4D9D4364D59C83B1E6DCA1B5361CF0E3731EE0CA76B3A56A1911F6D8AAF0AC7C29D6B1DAD420DFF75609555419C353CBA856898960CABDF64A106E5C6762 7C
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N. m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.2.6.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sun May 28 17:44:38 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	34732
Entropy (8bit):	2.0483473532441185
Encrypted:	false
SSDEEP:	192:5JF/5cU2HffnsHOeJVFmwYWlpVvqhl2gaDm9zE+92:vF7ae3FVCnvUAgBh2
MD5:	3EAA5D6004788F1705B23D25B290DA30
SHA1:	B37D26CA776713E07AFDAD07119ECE4FC1A864A0
SHA-256:	83EC7511035D33FAAB621D9D57D620977A01C64727C59D50438A4C3A5D2BE2A1
SHA-512:	C5D51E11898F44367381F1128A1C05112C3AD21532906C5FB84B5F819E8C245813F33EF25F6B4F6CAFADAF7CA6508A3C72A90F665815A1B8F0C3C382BD73B91F
Malicious:	false
Preview:	MDMP..... .....sd.....&.....T.....8.....T.....r.....U.....B.....8.....GenuineIn telW.....T.....t.....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\WER6C3A.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):	8372
Entropy (8bit):	3.7012302589385317
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNip86o6YBSWSUqgmfqSRWCpDZ89bT7sfXNxm:RrlsNii6o6YBTSUqgmfqSGTAfXS
MD5:	53F1B9224355CE1B37614F795623726B
SHA1:	2CD2084CAB253CF2BBAA3A264A618DD343EB3E1A
SHA-256:	29875BF32642661C10FA857DA81E9FB51D716D3F6E72BDA198A9323F6DE5B5B9
SHA-512:	80AF297CCFBB4D59B1CBB2512994EC78797E287D7E52DB5B57D3CAECC74D77D18E0FE21B01519232FC6D95A982A470C3D78FB47F17B25F38718DA1F7183762 C

Malicious:	false
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.>.4.7.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6CA9.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):	4.464714975972279
Encrypted:	false
SSDEEP:	48:cvIwSD8zsoJgtWI9aEWgc8sqYj08fm8M4JUATA6RjFeY+q8vzA6RiTA0JA0ad:ulTfuJdgrsqYVJUATAvYKzAnTA0JA0ad
MD5:	70253C5C49106077A9C723B3C4811D9D
SHA1:	77D295F3F2636F66547A6010B8A6A41749112D90
SHA-256:	51659FC604D5837AC7F0D8F551199610C8E7F8FC9A6D6EACBDE725174D702EAF
SHA-512:	3155FDD565D2AE866E9DDD7729A86F83B0E32BC9BFB6F56ED49982F91F6DE97F0930F05A70DEDF47779B1C094275E828DBF64E5185D1F94A85E9F47F83A1728
Malicious:	false
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="2060815" />.. <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:\ProgramData\Microsoft\Windows\WER\Temp\WER6CB6.tmp.csv

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	78304
Entropy (8bit):	3.0617993029431148
Encrypted:	false
SSDEEP:	768:+DHmBiA/EYWYF65NDD6orMmziLkRkKG55HF8jNJX:+DHmDpWYF65RrMmz4rKoHF6j
MD5:	9B00C3788ACE66D2813ABCF5395CC8E2
SHA1:	D3E96707C196134240B024BCD6872B058B8C3739
SHA-256:	36491EB0B120F1341D6E097896E8A92481248C31D840932E174EE2B252266BB4
SHA-512:	35850A7F4003B3775EDF08B4A48C8D17F731BFEAD37223073E2A9E22DAC38BE86A025F633D641668C85B30E0284A645024399DBCF9FDEC92466370B54291750E
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E3E.tmp.txt

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.696421435047623
Encrypted:	false
SSDEEP:	96:kiZYWnpIRStuEYYYAW9HVYEZvwKntk0ig4dzMwS1Q8UaG8H1sgIIOJ3:hZDnpr/LK/1qaG8H1sgvOJ3
MD5:	D405953F3601BF7BDB00BBB197B81340
SHA1:	CE527D6D54435044432CF0ACCD95D5234ADB3327
SHA-256:	99EB377629F384F1AB45393450C2B0D43335EABC9433AF5303905AB328FC17F6
SHA-512:	654795C0C20B8A6029FE484BE21743A14F73C155E4647A009354048912865B7D370D44799188A1DF93A8147F7F1BC40361A32FFB3021525770C1D436B1A0BACE
Malicious:	false

Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.2.6.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6B2.tmp.csv

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	82458
Entropy (8bit):	3.0522203435441395
Encrypted:	false
SSDEEP:	768:WcH/QbEv65rXhmlzez+7gOjoR2rZEiOR+Oz84:WcH4y65jhmlSzE5oRcZEiOR+Oz84
MD5:	43E6DB3836E17C8B26B851F018114E03
SHA1:	22F3CFB2E4564F7FE482093DACBA8BC48AB3621C
SHA-256:	1B881748199DABAC475143DCCC372542212278F33AC67B1507240651CD0268DD
SHA-512:	9FDD99035643A72FF953D9CDE9F115633161FFB1A680C14EB7D500962D8E22FC9C606CA1C7366CA74A355F72935336E78F3F85E6E2C98AF84BA726D5979664D1
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H. i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,. P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a. g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a. t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T. r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA9B.tmp.txt

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.696967017813337
Encrypted:	false
SSDEEP:	96:kiZYWq/WfsY8Y3WNpH8YEZenQt8iUsClczBwffWgav8HEquMVnInLJ3:hZDI7JnAPnav8HEquMCLJ3
MD5:	661A07BA18244360224E3C75D3E85AB4
SHA1:	4EA36E4954E42323A61923C29F1E8726490CCA71
SHA-256:	02CAB86C1C4641CD0EE19B8D7BE4AEEA94BECC0D0E2EA238E85A5DAC8D4090D9
SHA-512:	C71B23415FC0925DB5CB3B94F767DE6BFACED805A8300CE740AB650E0D4E534731BA0114EDD4B566272194C1E8319FFFE958C207A2EECA6765D166EE2C3468 0
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.2.6.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4D6.tmp.csv

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	82286
Entropy (8bit):	3.0523897811972973
Encrypted:	false
SSDEEP:	768:VEHpNIDEDft5oa6diZmlz6DnwO8w1rZEiORtuHYat:VEHTImft5oa6QmlW7GwhZEiOcYat
MD5:	AF19E87CE8A93DC5F83EC5EA52E945B3
SHA1:	8EA60ADB87A1E56673A6843184BFE8D82995A244
SHA-256:	F116ED6D77882BB3E97BA13C96414BB2B112FA70B31AC8B549F0B61D6931EB45
SHA-512:	0F9C173155D3614D3B92CEE82BBCF0D73F75ADBC4D9C7D9FC7A9C00BB66498EB313E2A9A3DCD4B54A354E34A762BC600FC8F00F246728109822DBFB076EDA E7
Malicious:	false

Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9E8.tmp.txt

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.699598390624135
Encrypted:	false
SSDEEP:	96:kiZYWYxRWNKYyYMkWOUHyYEZj+Dt8ih5oz5wWmTaU8H2R3yI5J3:hZDelY+wEaU8H2R3V5J3
MD5:	AB702085B616CE376B2EA315101D510E
SHA1:	C1DCB39DD0A41B4514FDD59CA3C298BA9412831F
SHA-256:	A71B8B7DD32E2E90B72E4F4BE61554189F71439672AC2A874F781459F29DBE29
SHA-512:	ECBD1C02E15C609D5A8B05AA21FFBF28218CAA9BAF4FB14832A99F398EDF15C74C4D0DEC5C6C4CD098CDACC83D7D8A2CDF410D759F05D351C787EC06A30 4DE3
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N. m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.2.6.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB41.tmp.csv

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	83508
Entropy (8bit):	3.0503607553509378
Encrypted:	false
SSDEEP:	768:y+HI7tEU9Tt5yc6diZmlztDQGTrO8ORrZEiOuMPzAoE0:y+HOf9Tt5yc6QmlxMGTvOtZEiOuyAoE0
MD5:	C8D3B5E032CC6386B8F0F98B86784072
SHA1:	C86BBBAED0293A6CE1D6823C8001341DE577130C
SHA-256:	6D4F4D1C866BCBCBB72D6CD4FEBA91C5A09670D9FD5B07EE223F20BB71533452
SHA-512:	2146271186E6E4B22D9D572F2D6576D9487754DF0EEB338C41F81A855B92225CE474D715AD949E2688822FEA49CABDBA9590E1DD5399A9E460A35E4051954348
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE6E.tmp.txt

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6992949384797567
Encrypted:	false
SSDEEP:	96:kiZYWOtTrUZYeYWWdoWHHYEZcKt8ie53zRwthUqsao8H1Tn3H4IjJ3:hZDOCptr4+fao8H1Tn3HfjJ3
MD5:	5EB6922F99FA343FD44D112AE19BB276
SHA1:	E2558547F8913774EAD8F4F1D685C024E36CBD0F
SHA-256:	7FE851DCDAE1FEE2ABFCAEECE51AE7CD6D8A3079EA796CABEEBBAE307BDF9DA4
SHA-512:	9F52C3A0A960064A1467BA49457B115357D8829A018597E9F461B100ACEB497C58B1B472B7AA4117B190AF808A9AFA2858C8976A9C8FD1894854FB5DDE48ED0A
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N. m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.2.6.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\SystemID\PersonalID.txt	
Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.963745994207334
Encrypted:	false
SSDEEP:	3:oTXoaMC45vn:2oDn
MD5:	0156D0C4447C9DC5F0995701DC91FB59
SHA1:	763CCC86E08AA791AD0E6085472518697535095F
SHA-256:	29E03691D1E3DB7DFB5542555DAECD4DDBC881033A574B28720401FC272B9E56
SHA-512:	D73D70CB6F3D6B647D39147902F8767A9645483FC1ED5D62E57232F47D6251A9BDF5AADFA447748F0E6DED8D2AC50FC5A632EDE00E8962C030C52D9853F219 E
Malicious:	false
Preview:	5MivdxIsjUGGGxmy4wa3GzTKau2fLCnJ4rWgvwBY..

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old	
Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	459
Entropy (8bit):	7.4061246314302585
Encrypted:	false
SSDEEP:	12:s/3TC9uNXd0ZdF00tXpHOnKUfw4v2ascii9a:k3TC9uNXd0ZdF0sXpHElfbD
MD5:	C4EC3BE085F7A89CC7623FF5E72690EF
SHA1:	A667CD7934485B094EDBB2D7D2D9082A406D3F8A
SHA-256:	C995B07A5C3D258807F33062D45B10081B71543FEC482AC8BE7D6C915417D17B
SHA-512:	D7CD172C88C33A33BF30ADAC4B9FD625314B45C7182A869A0305A2669C009CAEA1A92290E7E7119F5224F1FBD2383C6C371E81FD3005103E0582F85F97FAB97
Malicious:	false
Preview:	2019/.\`.....I ...W..i.....&k.~4s..$Jz....a...N.....`iw-.v`...<..!...y.}.8v.. F..B.....$B..3OB0xmR$U...u.../.....;aM.....Y.!K..y~#SY$y,..B3.....YrXW...f.sN.S..Rq..Q..Y..hftXF R...1..gUQ..4.. .\..4... ....WN.}b.9.....L.-.).i(.....e.D.....+...y.,.kJ..^..... ...t.....%.c...z[u..(..bs.....A..;.....`8N.M.,.rV.n.,..wH..WID....9^.....wN#Y..(..:.....?.DMS.3.`qJ5Mivdx IsjUGGGxmy4wa3GzTKau2fLCnJ4rWgvwBY{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\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	459
Entropy (8bit):	7.4061246314302585
Encrypted:	false
SSDEEP:	12:s/3TC9uNXd0ZdF00tXpHOnKUfw4v2ascii9a:k3TC9uNXd0ZdF0sXpHElfbD
MD5:	C4EC3BE085F7A89CC7623FF5E72690EF
SHA1:	A667CD7934485B094EDBB2D7D2D9082A406D3F8A
SHA-256:	C995B07A5C3D258807F33062D45B10081B71543FEC482AC8BE7D6C915417D17B
SHA-512:	D7CD172C88C33A33BF30ADAC4B9FD625314B45C7182A869A0305A2669C009CAEA1A92290E7E7119F5224F1FBD2383C6C371E81FD3005103E0582F85F97FAB97
Malicious:	false
Preview:	2019/.\`.....I ...W..i.....&k.~4s..$Jz....a...N.....`iw-.v`...<..!...y.}.8v.. F..B.....$B..3OB0xmR$U...u.../.....;aM.....Y.!K..y~#SY$y,..B3.....YrXW...f.sN.S..Rq..Q..Y..hftXF R...1..gUQ..4.. .\..4... ....WN.}b.9.....L.-.).i(.....e.D.....+...y.,.kJ..^..... ...t.....%.c...z[u..(..bs.....A..;.....`8N.M.,.rV.n.,..wH..WID....9^.....wN#Y..(..:.....?.DMS.3.`qJ5Mivdx IsjUGGGxmy4wa3GzTKau2fLCnJ4rWgvwBY{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\4DDQNYCN\www.msn[1].xml	
Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	347
Entropy (8bit):	7.366556587581152
Encrypted:	false
SSDEEP:	6:c7PIlJSBjQRclyxQNVRGUmfv3jEfnS2kNkZHgfAIoyascii96Z:c7AlSjQRZSVRG93462kNuIascii9a

MD5:	CD2031C3A7797C0BE2DCE03F8C559A36
SHA1:	5B60AA2C6490B0A072ACC52EDDA4372D4981580D
SHA-256:	769203F17380C1AD513EEEE58CE7E0201F8B9A2069840BE2788DE83C04A5CE12
SHA-512:	132D116B623D0EBF776373B99F61E0D4C12E2C5A483060193E32E6E47D5AFA94AF7C8452D5BBCCB9A321449E76E6F4B1A2B8A2D3FD232F30933BD2DFF3D860 1
Malicious:	false
Preview:	<root.....Q.Q...=L./k....t.[.R).L.*....6C".w.....E.^?.!..T&(.....=#.`....}.N..]..S.F5tWy<J.%.....6.. ...s.#.r..}g.D.0}=.'.#..S.O.j..:....|88..w2j.V."......9M...:..$..Pz....!..{...H.."R...:Y.? ^...e.vr!..l~..e.}:'.).5..e1.b.....k._...06..'..e..f...\n..c5MivdxIsjUGGGxmy4wa3GzTKau2fLCnJ4rWgvwBY{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\4DDQNYCN\www.msn[1].xml.vapo (copy)

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	347
Entropy (8bit):	7.366556587581152
Encrypted:	false
SSDEEP:	6:c7PIlJSBjQRclyxQNVRGUmfv3jEfnS2kNkZHgfAIoyascii96Z:c7AISjQRZSVRG93462kNuIascii9a
MD5:	CD2031C3A7797C0BE2DCE03F8C559A36
SHA1:	5B60AA2C6490B0A072ACC52EDDA4372D4981580D
SHA-256:	769203F17380C1AD513EEEE58CE7E0201F8B9A2069840BE2788DE83C04A5CE12
SHA-512:	132D116B623D0EBF776373B99F61E0D4C12E2C5A483060193E32E6E47D5AFA94AF7C8452D5BBCCB9A321449E76E6F4B1A2B8A2D3FD232F30933BD2DFF3D860 1
Malicious:	false
Preview:	<root.....Q.Q...=L./k....t.[.R).L.*....6C".w.....E.^?.!..T&(.....=#.`....}.N..]..S.F5tWy<J.%.....6.. ...s.#.r..}g.D.0}=.'.#..S.O.j..:....|88..w2j.V."......9M...:..$..Pz....!..{...H.."R...:Y.? ^...e.vr!..l~..e.}:'.).5..e1.b.....k._...06..'..e..f...\n..c5MivdxIsjUGGGxmy4wa3GzTKau2fLCnJ4rWgvwBY{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

C:\Users\user\AppData\Local\205aa591-8aa8-4e2c-a5b1-c9b7aaf860cf\build2.exe

Process:	C:\Users\user\AppData\Local\Temp\BDC0.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:	7D5BFC95C8F3D5BCC12A4AE1929B4FF946AB3747B29B3AB57B684DECFA78DB4836EC187D8A9ECDA5D2E6C4BAA02989AC1648FB9AAA0E592FB3A70F880529 E3A8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 87%
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\205aa591-8aa8-4e2c-a5b1-c9b7aaf860cf\build3.exe

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
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\Local\205aa591-8aa8-4e2c-a5b1-c9b7aaf860cf\build3.exe, Author: Joe Security • Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: C:\Users\user\AppData\Local\205aa591-8aa8-4e2c-a5b1-c9b7aaf860cf\build3.exe, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: C:\Users\user\AppData\Local\205aa591-8aa8-4e2c-a5b1-c9b7aaf860cf\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\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.exe

Process:	C:\Users\user\AppData\Local\Temp\BDC0.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\Microsoft\CLR_v4.0_32\UsageLogs\223E.exe.log

Process:	C:\Users\user\AppData\Local\Temp\223E.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\B87Z87FM\build2[1].exe

Process:	C:\Users\user\AppData\Local\Temp\BDC0.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\B87Z87FM\build3[1].exe

Process:	C:\Users\user\AppData\Local\Temp\BDC0.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\B87Z87FM\build3[1].exe, Author: Joe Security • Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\build3[1].exe, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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\B87Z87FM\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\B87Z87FM\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\B87Z87FM\cred64[1].dll, Author: Joe Security • Rule: OlympicDestroyer_1, Description: OlympicDestroyer Payload, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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.....p.....text..... ..`.rdata.....@..@.data....o.....6...|..... ....@....pdata.....@..@_RDATA.....J.....@..@.rsrc.....L.....@..@.reloc..h.....N.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\get[1].htm

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	560
Entropy (8bit):	5.993855904320204
Encrypted:	false
SSDEEP:	12:YGJ68UisWA3za2fvVv4iW758vgMnzFvnt2sJsskUO55B:YgJUileztGd58IozFv0sJsskUEr
MD5:	3ED26AD1EC88691BA5D2284C38622F49
SHA1:	371E407D2246876759AD04F42DACEB653F417EE3
SHA-256:	EB0A596BD847FE153EB4829616CB63A2939E3C6E3CAAFF0DCEAAE17BAD3B1935
SHA-512:	5469B03E6D0D25FE62844CD3B5BB447252C6076ED486AEF5D33F3679E3DC65201D91D1CF00891446AFC67E09CE75548201877D0A9F8CCE52227BCC1D615883E
Malicious:	false
Reputation:	unknown
Preview:	{"public_key":"-----BEGIN PUBLIC KEY-----\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzo\/R71k\/vaNVynBPEMMp\\nVG7sEXmhuiIxTytGA vF1BeGhEiNJ34cqeIsppM7ZOEsOLuS6zVrL7YTuj359KqAN\\nYwCRLcioIpPrdUnmvFcY\/i0bLAfSShy0IYhcTIPimQ0O6Os8V7V\/nwkPwF0ppIz7\\ne5EKUeiwjI5 p+r+FYzqNWVhBQv+q7prsPgdKtyY62bZ2W8QVWI8\/fkt3FcsoXTGy\\n0irp1p5JSA36OvzvnE0cXe6IT6vPZ5BKXSPUaiHxEFA9drGCzsQFY8JwhvJEMuFS\\nX5bazS rBMsy+0N8Zg+vClZYAVkoFuSN\/gPKDuWrOHBJdcERVFJ05yZTTZwTJXGxx\\nxwIDAQAB\\n-----END PUBLIC KEY-----\\n","id":"5MivdxIsjUGG Gxmy4wa3GzTKau2fLCnJ4rWgvwBY"}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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...}....l|....S..>.....aRW;~g..y.l4_).....)...(v.w.....]2.k}>P...^...|..=.c.u...V

C:\Users\user\AppData\Local\Temp\110C.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\223E.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\223E.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\4445.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\4445.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\5B59.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:sdhlITZXaG2MjEkQyX7ev9DgST8jIgxATGG56aETtiE: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\6A3D.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\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.....@..@.reloc...*.....,.....@..B..... .....

C:\Users\user\AppData\Local\Temp\740E.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**
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\7439.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: 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\78BB.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\78BB.exe, Author: ditekSHen
Antivirus:	• 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\794C.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+l
MD5:	15BC205C2CAF7196EE2267087C3B2BB8
SHA1:	0E1EE7E4CCAFD5A62D6B2B3A9369709EAB0E1F0B
SHA-256:	FDEE1B99A95C5DFB4A256CDB7E43CE3F21A5D2C2977CE252AAFFA77A9E017DDF
SHA-512:	DBFD1C50D16F21084B542A2ABD2B35F6489D30B55E9B5B8DC9014BCC9C4AE8A24DF08A659B28EAD862291BC65107A34C0CDA8CAD08A354E92FA23138D21F62C
Malicious:	**true**
Antivirus:	• 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\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):	87584
Entropy (8bit):	7.905083202118323
Encrypted:	false
SSDEEP:	1536:C0APYRogokY91WKpMOyVPOBxVwYT49KmMT0guMWlnyU7h/DD/Pjgok4pFwOUpYOb:tToT+KdUOB770UYguJyGtPjbeOUaOHpl
MD5:	51C8EE42F5DD3B1A795BB108648730D9
SHA1:	DB0A1B54392C8DD8FD33220AEFB02B8752BACDFE
SHA-256:	989B73040C9E092B508EB82AADDF5D3B695FD000BD0EB09771997A8C8F2B0349
SHA-512:	D5CDE42AA9E2B42437A57CD4D43BE0FFE1B65BD9F627208DACC7D6F600B06CCDDFF55A232372EF1EFB6889B824A69927A456D336E9AC1D94D2786DD5E6746E16
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`.....C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222...........".................... ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....w........!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....?..01KK...lq\....xcS.m..#Hm.....T......<!...wq5...v1.?S.....rHj-.U:...5............\|..+.......}...<.>...H.......Wo.CK`/l.1./...C...W.....,1....R.0.W.M.!.l7.~S....."SW.^..c......^s........u,-n....A..?.2.....l.(.?....7..~.q$.f..1\.q[.....oS:.gOY".....f-%.P.b.Z....>.....4+..b.Y&..F...)Pq.L....... .....H.#.|..).?.H.'.|....).?m.....h.t......|4.%......

C:\Users\user\AppData\Local\Temp\8DD2.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+l
MD5:	15BC205C2CAF7196EE2267087C3B2BB8
SHA1:	0E1EE7E4CCAFD5A62D6B2B3A9369709EAB0E1F0B
SHA-256:	FDEE1B99A95C5DFB4A256CDB7E43CE3F21A5D2C2977CE252AAFFA77A9E017DDF
SHA-512:	DBFD1C50D16F21084B542A2ABD2B35F6489D30B55E9B5B8DC9014BCC9C4AE8A24DF08A659B28EAD862291BC65107A34C0CDA8CAD08A354E92FA23138D21F62C
Malicious:	**true**
Antivirus:	• 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\946D.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**
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\AD22.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**
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\AFA6.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:	DBFD1C50D16F21084B542A2ABD2B35F6489D30B55E9B5B8DC9014BCC9C4AE8A24DF08A659B28EAD862291BC65107A34C0CDA8CAD08A354E92FA23138D21F6 2C
Malicious:	**true**
Antivirus:	• 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\BDC0.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**
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\C45B.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: 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\D789.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**
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\DC0A.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**
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\EB26.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\EB26.exe, Author: ditekSHen
Antivirus:	• 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\ECED.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**
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\F0C7.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: 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\NewPlayer.exe

Process:	C:\Users\user\AppData\Local\Temp\223E.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.....@..@.reloc...*.....@..B..... .....

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

Process:	C:\Users\user\AppData\Local\Temp\223E.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\223E.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\BDC0.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	560
Entropy (8bit):	5.993855904320204
Encrypted:	false
SSDEEP:	12:YGJ68UisWA3za2fvVv4iW758vgMnzFvnt2sJsskUO55B:YgJUileztGd58lozFv0sJsskUEr
MD5:	3ED26AD1EC88691BA5D2284C38622F49
SHA1:	371E407D2246876759AD04F42DACEB653F417EE3
SHA-256:	EB0A596BD847FE153EB4829616CB63A2939E3C6E3CAAFF0DCEAAE17BAD3B1935
SHA-512:	5469B03E6D0D25FE62844CD3B5BB447252C6076ED486AEF5D33F3679E3DC65201D91D1CF00891446AFC67E09CE75548201877D0A9F8CCE52227BCC1D615883E
Malicious:	false
Reputation:	unknown
Preview:	{"public_key":"-----BEGIN PUBLIC KEY-----\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzo\/R71k\/vaNVynBPEMMp\\nVG7sEXmhuilxTytGA vF1BeGhEiNJ34cqeIsppM7ZOEsOLuS6zVrL7YTuj359KqAN\\nYwCRLcioIpPrdUnmvFcY\/i0bLAfSShy0lYhcTIPimQ0O6Os8V7V\/nwkPwF0pplz7\\ne5EKUeiwjl5 p+r+FYzqNWVhBQv+q7prsPgdKtyY62bZ2W8QVWI8\/fkt3FcsoXTGy\\n0irp1p5JSA36OvzvnE0cXe6IT6vPZ5BKXSPUaiHxEFA9drGCzsQFY8JwhvJEMuFS\\nX5bazS rBMsy+0N8Zg+vClZYAVkoFuSN\/gPKDuWrOHBJdcERVFJ05yZTTZwTJXGxx\\nxwIDAQAB\\n-----END PUBLIC KEY-----\\n","id":"5MivdxIsjUGG Gxmy4wa3GzTKau2fLCnJ4rWgvwBY"}

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:qVoB3tUROb0b0qHXboAcMBXqWrKb0GkIIVLLPROZ/eIwcWWGu:q43tIkObRHXiMIWObtkII5LPROeIpfGu
MD5:	1B7C22A214949975556626D7217E9A39
SHA1:	D01C97E2944166ED23E47E4A62FF471AB8FA031F
SHA-256:	340C8464C2007CE3F80682E15DFAFA4180B641D53C14201B929906B7B0284D87
SHA-512:	BA64847CF1D4157D50ABE4F4A1E5C1996FE387C5808E2F758C7FB3213BFEFE1F3712D343F0C30A16819749840954654A70611D2250FD0F7B032429DB7AFD2CC5
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:	5AF414C95DB738D0A65FDD67F2FF3923C451EE68856237F55626586AAC14EFE62288F5B8D74A5FBF2EABA9E6A1689CEA89B856212A597AB12A3A4B0097E3F3A5
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\cuwsgii

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	282112
Entropy (8bit):	6.603075701960206
Encrypted:	false
SSDEEP:	3072:kKAuVGwBlcQlbzjmj7FHmfuzv+ippcQPd5gG+LGvAcYWt:9AuVGhQlbzUw+5XcPGmvW
MD5:	6017E7C6F19DE9E3B0AAE0965FE25603
SHA1:	605250B6DABAFB86252272B757A1713078C6AE79
SHA-256:	C421418B410EA4BF78EF47C8EDB75C8FC96220043573BA6D8268BCA900A4C041
SHA-512:	DA62CAB044A336881F388E93495ED9BC6AA6D1559556DE0EFE8585B932A3E12C7A20322E913FB0FA8B3C402B119D5924EFC6FE51550AC95C2967713A0B0B0ED1
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 38%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...|.....|.....|...H...EX..k...b.....|...c...|...c...|...c...Rich b.....PE..L.....b.....&.....M.....@.....(.....d....&..w.....p(..... .....0..@..... .....text...b~..... ..`.data...DX$.....@....rsrc....w....&..x.....@..@.reloc...3...p(..4.....@..B.....

C:\Users\user\AppData\Roaming\cuwsgii: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\AppData\Roaming\vwwsgii

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\Desktop\EIVQSAOTAQ.docx

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.8652538312624705
Encrypted:	false
SSDEEP:	24:R0TbuIYG9dbqACEctqItj6ME1eYkAAeGHDqgC3fdmKswSNinSdJZi+BaapcatGbD:suIn27/B6MWe7AAeWDJpwSNiSzZi+QGK
MD5:	9524737E3C462358FC445D6F5E2CDFB7
SHA1:	FC46ADA29CD8788FEE3D28E6ED96400481E91813
SHA-256:	92978C924E15848652C972B2F21EA963ABED234D257B41FB97C60E7EEE4331A7
SHA-512:	154662B7F8C754AC95D6F8F1CDFD74C3E899ACC5C91DBAD15C2882E5D7621BA279A7E0945D18AFF0DFE9F6032F3D331E76B108BD48571AA73F5C67D17D9635A
Malicious:	**true**
Reputation:	unknown
Preview:	EIVQS./P.(....r...)S..zc.>.j.n2 ...>.&.b2..KA....i(..1a....5.M.](..)w.....^.&="..mT... I.X.h..\...gZE.p.....V.R.....dG.U;\.M$.B..\|...tH...p.....-K.^.1...+.+>.}.h..F..u...{d.$:39.a.[.7... ....`.....Ly.^.w.z.q.h..c2...../.....M..).t.....d...G../..4..t....w.....a..|...y..i.&.1/...o..r.0.....3!.&*....-.../.o."..j.7...j!.na.....[.'.....m}..*2.....}..4..`.]...xONq..-..}.....t6.[,_..=J.N*. ..m.4w\x@.6Y.....*..#.L..V.g..T.S.Js*...i..GzT)..Q.o.7... .K..K.2r0.XH.z...:t...=.6..5.EV.S..v3.g...E./...v.#.....]..._.d.....W.e...y.l....M...u....TeJ.+...4....X.}...>.^..M..bB.9...H..f". R...T.....J.h$.H.....F.....P]..^3.o,...gQ.<2C...@..).....`7.@....i.....P..R..=.....&.z..(@P.,.....ijv..C&%...$..*/..ta..X....h.....P.....`...F!.....<\.Eq0?..^..4...M.....\.....s^...L...-....W?..J..n...$m.0.....y9.J.C.....t{G..U+D.:..2jqq.}.....4_.#..1.-.^Ds.....)...h.....3.h.n..|.Z...@_.....@V....v.w.N...

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.8652538312624705
Encrypted:	false
SSDEEP:	24:R0TbuIYG9dbqACEctqItj6ME1eYkAAeGHDqgC3fdmKswSNinSdJZi+BaapcatGbD:suIn27/B6MWe7AAeWDJpwSNiSzZi+QGK
MD5:	9524737E3C462358FC445D6F5E2CDFB7
SHA1:	FC46ADA29CD8788FEE3D28E6ED96400481E91813
SHA-256:	92978C924E15848652C972B2F21EA963ABED234D257B41FB97C60E7EEE4331A7
SHA-512:	154662B7F8C754AC95D6F8F1CDFD74C3E899ACC5C91DBAD15C2882E5D7621BA279A7E0945D18AFF0DFE9F6032F3D331E76B108BD48571AA73F5C67D17D9635A
Malicious:	false

Reputation:	unknown
Preview:	EIVQS./P.(....r...)S..zc.>.j.n2 ...>.&.b2..KA....i(..1a....5.M.](..)w.....^.&="..mT... I.X.h..\...gZE.p.....V.R.....dG.U;\.M$.B..|...tH...p.....-K.^.1...+.+>.}.h..F..u...{d.$:39.a.[.7... ....`.....Ly.^.w.z.q.h..c2......./.....M..).t.....d...G../..4..t....w.....a..|...y..i.&.1/...o..r.0.....3!.&*....-.../.o."..j.7...j!.na.....[.'.....m}..*2.....}..4..`.]...xONq..-..}.....t6.[,_..=J.N*. ..m.4w\x@.6Y.....*..#.L..V.g..T.S.Js*...i..GzT)..Q.o.7... .K..K.2r0.XH.z...:t...=.6..5.EV.S..v3.g...E./...v.#.....]..._.d.....W.e...y.I....M...u....TeJ.+...4....X.}...>.^..M..bB.9...H..f". R...T.....J.h$.H.....F.....P]..^3.o,...gQ.<2C...@..)....`7.@....i.....P..R..=.....&.z..(@P.,.....ijv..C&%...$..*/..ta..X....h.....P.....`...F!.....<\.Eq0?..^..4...M.....\.....s^...L...-....W?..J..n...$m.0.....y9.J.C.....t{G..U+D.:..2jqq.}.....4_.#..1.-.^Ds.....)...h.....3.h.n..|.Z...@_.....@V....v.w.N...

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.836915818342894
Encrypted:	false
SSDEEP:	24:Rlg8pVBz7mXpyr3Gx2z+ESEXyp7NRNrKyaCEFSZKMG0htjzneaCi1ZnQGtwbD:PpVFTTGkgEXSfNrTEFGKiNVCoZnQGcD
MD5:	C43A44569729CCFB186A75DE9B08DA59
SHA1:	E4D7C37C476B25E408A5A5200B9F1FF2F6BC9687
SHA-256:	EEA448DC6B199FDAA7534B2AF958FDE88D7E513C7E9A1E3F7E0DCBA66C7C1473
SHA-512:	1841E321B9249B6CE9CBBFEF5F75894C63CBC888BE522E50ADCC34F87D1603AEBA0D1927CA724CEA6DA44483C79627CE74E7057A7F5157F775BB8613085232 9
Malicious:	false
Reputation:	unknown
Preview:	EIVQS.W9...W..c*<...T.....m.5k..^s.nS..Hh{..q.....b...-?.g...(.....Z.,.j.-.b..STm.P...3.{..&H..U...c`7.....&..:+..M..9.^6...C._...;.*...<~....vq.Z..6&C.p...}&...s*....A....@H..h.....$.G ..5e*"n..\.....Bf.q1(.Y.s...T.B.3w..0...iz.....G...._.54..V.g...]...QSU...c..=R...:4....V.]..i!.c...%.g...!=.Y.U.CK.....)Y.KY..?ej..N....S...\..s.Gy9.qB...i..>=u;...&..Y.....}..{..8..WJ.....].... .W6...~.Zl.-.*.c....K.....?.{...]V...N..U.kw.e6j|.,hy...-..c.Fig....X..`.'...^.,.q.j<.....M..<...b....y..}.+.M....H.~S.....r9.:.:P.5..-?./.t9...h.L.Y...*..I.S'.kr...^v....%.hn..-`Xx.aB-._..\<R...z..w. (... z..S%.K...EOv..Q.1.#..5{.0V....&j..a3l..C.,8.....C..oV_...Z..T....5.L.IR.q~q..1..P.::.F.....8.e....E...xdF.....5.....Q)G.<..n..}...|..SBE..A..K.&..U..|Z...cDGs..O.....!].G.~..I....n< ...V.2.hx."...ph[.M..fz.....zx.4.(."...Pn_..... j.}.....I..!&E^.X..,.k.....H....A.J..0A.tu.d:Tc\|e..uc..[,..B`..._..^.&q...$.....p..$....?.....i..?s...kO..I.*..A.^...\

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.836915818342894
Encrypted:	false
SSDEEP:	24:Rlg8pVBz7mXpyr3Gx2z+ESEXyp7NRNrKyaCEFSZKMG0htjzneaCi1ZnQGtwbD:PpVFTTGkgEXSfNrTEFGKiNVCoZnQGcD
MD5:	C43A44569729CCFB186A75DE9B08DA59
SHA1:	E4D7C37C476B25E408A5A5200B9F1FF2F6BC9687
SHA-256:	EEA448DC6B199FDAA7534B2AF958FDE88D7E513C7E9A1E3F7E0DCBA66C7C1473
SHA-512:	1841E321B9249B6CE9CBBFEF5F75894C63CBC888BE522E50ADCC34F87D1603AEBA0D1927CA724CEA6DA44483C79627CE74E7057A7F5157F775BB8613085232 9
Malicious:	false
Reputation:	unknown
Preview:	EIVQS.W9...W..c*<...T.....m.5k..^s.nS..Hh{..q.....b...-?.g...(.....Z.,.j.-.b..STm.P...3.{..&H..U...c`7.....&..:+..M..9.^6...C._...;.*...<~....vq.Z..6&C.p...}&...s*....A....@H..h.....$.G ..5e*"n..\.....Bf.q1(.Y.s...T.B.3w..0...iz.....G...._.54..V.g...]...QSU...c..=R...:4....V.]..i!.c...%.g...!=.Y.U.CK.....)Y.KY..?ej..N....S...\..s.Gy9.qB...i..>=u;...&..Y.....}..{..8..WJ.....].... .W6...~.Zl.-.*.c....K.....?.{...]V...N..U.kw.e6j|.,hy...-..c.Fig....X..`.'...^.,.q.j<.....M..<...b....y..}.+.M....H.~S.....r9.:.:P.5..-?./.t9...h.L.Y...*..I.S'.kr...^v....%.hn..-`Xx.aB-._..\<R...z..w. (... z..S%.K...EOv..Q.1.#..5{.0V....&j..a3l..C.,8.....C..oV_...Z..T....5.L.IR.q~q..1..P.::.F.....8.e....E...xdF.....5.....Q)G.<..n..}...|..SBE..A..K.&..U..|Z...cDGs..O.....!].G.~..I....n< ...V.2.hx."...ph[.M..fz.....zx.4.(."...Pn_..... j.}.....I..!&E^.X..,.k.....H....A.J..0A.tu.d:Tc\|e..uc..[,..B`..._..^.&q...$.....p..$....?.....i..?s...kO..I.*..A.^...\

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.851210798678752
Encrypted:	false
SSDEEP:	24:RwJv6MHjpp5+ZLr1mDTyp4Ze8Llq5YOabmqKPddxgMoNae6cJjRKOPSU4kLHbD:KBbHjppUV1bALlCYNmqKPaMaaeLtaTs3
MD5:	F8F2C1A8F4BC43CA8DC31DDE9B42D5D2
SHA1:	2A0A1F94580D6E834EAC57AAD222CDB55ABC610B
SHA-256:	8FD963F80D5C6709071E95C5EBD1DF561EC0617B03BF92CB5DBCF207C659B396
SHA-512:	96794F594C01CB9A83D2F60A37BE7C968AF4A2929C6629B49B35BF7D94538F2C25E8716522C9DCA414E90F805B1A92A586A795BE210DCC0E4796F12F8DA697D
Malicious:	false
Reputation:	unknown

Preview:	EIVQS=.....v..9,..1M.;.L<>..9..(.U.Z.....~.9.V...+.....")-m$.....q..gA....w..K...._W-....j..^.O....\.....l]d.F..=?#L.d}?..yi..eu..%....@..z.9....8...K.$.V.6^. ..9..BF..Zg....m.\..".. "i...b....Yq..i..E.R.....XB.Z..... qh..w'.$.d.....Im...&..H.I.T.CW.jC.....oc...."D.U.9..J~%? .).:...HA...w..6...u;.9.d.9YWpUL....n;v..?...]X.O.V...R*.)J..Pk.!..A.U?.....5.v .T.N.A8.@~...C....j+B.n.c:.E_\R....A.....#4.....R..O.....^..YG"....@.nb).}.a..A.=.N..R....).:...8J..Z...%<.....?-.0.3..nZpU..,|.=^.@Y..1..D&`.].B.#0.6.....d....9...q.....j...K5....L5.C ...$m.k....ZxC.!_...~wc.D..H.-(.j..a..R...R. k...[&..C.N.Z.....O..D..v~}<.....n.<.W.).I.....d.....5..+...P.^.....U.0a.k/8.(.V.n.TC.:Yk.B...ZK*.&#.9G.m..)N. .fg..g]..C1'...VL.....~..M2 ....~...9^...@$....*0.Q...J...I\.....i./_Y'....!.A..`.x.<.o.Vq..I...9.XT..PDr.....W.?.....{.....0._....Q.&..T.g....y.i.S.W9.....%..$.H...~.....z.+8<...|..t.js...|W..{.P}*y!O....!!....`$9

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.851210798678752
Encrypted:	false
SSDEEP:	24:RwJv6MHjpp5+ZLr1mDTyp4Ze8Llq5YOabmqKPddxgMoNae6cJjRKOPSU4kLHbD:KBbHjppUV1bALlCYNmqKPaMaaeLtaTs3
MD5:	F8F2C1A8F4BC43CA8DC31DDE9B42D5D2
SHA1:	2A0A1F94580D6E834EAC57AAD222CDB55ABC610B
SHA-256:	8FD963F80D5C6709071E95C5EBD1DF561EC0617B03BF92CB5DBCF207C659B396
SHA-512:	96794F594C01CB9A83D2F60A37BE7C968AF4A2929C6629B49B35BF7D94538F2C25E8716522C9DCA414E90F805B1A92A586A795BE210DCC0E4796F12F8DA697D
Malicious:	false
Reputation:	unknown
Preview:	EIVQS=.....v..9,..1M.;.L<>..9..(.U.Z.....~.9.V...+.....")-m$.....q..gA....w..K...._W-....j..^.O....\.....l]d.F..=?#L.d}?..yi..eu..%....@..z.9....8...K.$.V.6^. ..9..BF..Zg....m.\..".. "i...b....Yq..i..E.R.....XB.Z..... qh..w'.$.d.....Im...&..H.I.T.CW.jC.....oc...."D.U.9..J~%? .).:...HA...w..6...u;.9.d.9YWpUL....n;v..?...]X.O.V...R*.)J..Pk.!..A.U?.....5.v .T.N.A8.@~...C....j+B.n.c:.E_\R....A.....#4.....R..O.....^..YG"....@.nb).}.a..A.=.N..R....).:...8J..Z...%<.....?-.0.3..nZpU..,|.=^.@Y..1..D&`.].B.#0.6.....d....9...q.....j...K5....L5.C ...$m.k....ZxC.!_...~wc.D..H.-(.j..a..R...R. k...[&..C.N.Z.....O..D..v~}<.....n.<.W.).I.....d.....5..+...P.^.....U.0a.k/8.(.V.n.TC.:Yk.B...ZK*.&#.9G.m..)N. .fg..g]..C1'...VL.....~..M2 ....~...9^...@$....*0.Q...J...I\.....i./_Y'....!.A..`.x.<.o.Vq..I...9.XT..PDr.....W.?.....{.....0._....Q.&..T.g....y.i.S.W9.....%..$.H...~.....z.+8<...|..t.js...|W..{.P}*y!O....!!....`$9

C:\Users\user\Desktop\EIVQSAOTAQ\HMPPSXQPQV.mp3

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.8798368452114085
Encrypted:	false
SSDEEP:	24:laS1aaDTCbsS8cK+DP32pGmBmClPh9QMwP8m/a7lCpOnX75sfmmu5Gb7Pcf9/ctP:ljgnK7MClPhCMMMjy1+vRb7G9/ctUG1D
MD5:	888B460D80B8D7E7238448ACD37B116B
SHA1:	5CEFF2CA2997DB1CBFA4E236AED39B6D60E95D74
SHA-256:	0143D33B1A2B933B825F9225220251D6276B3CFAE934A81CF30D1D3D9B272B98
SHA-512:	0057080537042619D4A4F1843AF66D21BCA1E19E529F809FC9583B78BF00E361497967E4F59B5965691D8FAC0AA560E7A9483393337827F831D3A4B6A32871B6
Malicious:	false
Reputation:	unknown
Preview:	HMPPS...l.x*g.Ol.+.&.K.&.q...=....g.q....x.D.hP...(e.....?...9X.X ...o*.-..8..FXA..u...[.-S...rIm..y........9....]...|.j.....|.."..2..8.-mT|.2,..$m.(.....m~...ssK..3|.9..<.#...x....>.?K.O... .K.B.s..O.....+S.d_..j.m....M._....E..-.S.V.`.r.2&.50....>..."........\.....=...1YA`..Je'..AZ...b..V.!.}.@e...<........6.Z...d.g...y.E..\......P..]...n.....^..,Zg..]D.....i..Uk...........&U.m!.7K...- ^...8..C2.../......7....4..)._.J..V...a.-.R.x`AG.ki..c[Y..k...N...T.....Z.@v>...u....(..K..E.F...9/...c.....2_.5[...N...../..k........[;k.Q...3....Y..Z..].7..'..*#..../..g.n.R.7.q.pY.....;[....._. ..Z%.....@..IO..T.:.`..gd-Q..(..9...k....N2.....:.....|c....9.~d..jvO....i.d...w.....\.....#H.#.Ii.....T.q./..%..T..8.<.#.VR.....h.;wVj.K..B..[d..e\..:-..q.L..N5D...f..x..z....nV...r.A.z. ..@..j..%..9.8.....z.....x#.............zR....4.3.}.aC...WX<.....A.q..Brb...N..zS#R|.<.o..?.|{.t....|...'.d.ae;b.'.x.....f.`...].+..I.....>...$....,.M

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.8798368452114085
Encrypted:	false
SSDEEP:	24:laS1aaDTCbsS8cK+DP32pGmBmClPh9QMwP8m/a7lCpOnX75sfmmu5Gb7Pcf9/ctP:ljgnK7MClPhCMMMjy1+vRb7G9/ctUG1D
MD5:	888B460D80B8D7E7238448ACD37B116B
SHA1:	5CEFF2CA2997DB1CBFA4E236AED39B6D60E95D74
SHA-256:	0143D33B1A2B933B825F9225220251D6276B3CFAE934A81CF30D1D3D9B272B98
SHA-512:	0057080537042619D4A4F1843AF66D21BCA1E19E529F809FC9583B78BF00E361497967E4F59B5965691D8FAC0AA560E7A9483393337827F831D3A4B6A32871B6
Malicious:	false
Reputation:	unknown

Preview:	HMPPS...l.x*g.Ol.+.&.K.&.q...=....g.q....x.D.hP...(e.....?...9X.X ...o*.-..8..FXA..u...[.-S...rIm..y.....9....]...|.j.....|..".2..8.-mT|.2,..$m.(.....m~...ssK..3|.9..<.#...x....>.?K.O... .K.B.s..O.....+S.d_..j.m....M._...E..-.S.V.`.r.2&.50....>..".....\.....=...1YA`..Je'..AZ...b..V.!.}.@e...<.....6.Z...d.g...y.E..\.....P..]...n.....^..,Zg..]D.....i..Uk.....&U.m!.7K...-^...8..C2../.....7....4..)._..J..V...a.-.R.x`AG.ki..c[Y..k...N...T.....Z.@v>...u....(..K..E.F...9/...c.....2_.5[...N...../..k.....[;k.Q...3....Y..Z..].7..'..*#..../..g.n.R.7.q.pY.....;[....._. ..Z%.....@..IO..T.:.`..gd-Q..(..9...k....N2.....:.....|c....9.~d..jvO....i.d...w.....\.....#H.#.Ii.....T.q./..%..T..8.<.#.VR.....h.;wVj.K..B..[d..e\..:-..q.L..N5D...f..x..z.....nV...r.A.z. ..@..j..%..9.8.....z.....x#.............zR....4.3.}.aC...WX<.....A.q..Brb...N..zS#R|.<.o..?.|{.t....|...'.d.ae;b.'.x.....f.`...].+..I.....>...$....,.M

C:\Users\user\Desktop\EIVQSAOTAQ\KLIZUSIQEN.xlsx

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.843706691982694
Encrypted:	false
SSDEEP:	24:bMM+pr6jqg0JJxXc+bYHBBiOmHEB7NMPnk+ThgJy0/6niIPDbK4UzbFRMbD:p4kqg0JvceYHviO9+TSl/WiIPi4kID
MD5:	E48313B62F0FFA8D166E313D1508E3FB
SHA1:	6BF900328C7CE54CAFFCC6C90C6FDA33CBCAE594
SHA-256:	6918E86999BBC902192C83A6FC91D5E43233B1E1330DE3E3BF123A0C9F47A173
SHA-512:	7D403D47969F8ACF2CA8F06E39B1A6BADF06A58EBA3ADB0E69BCC82D3AD9666B10809A808ACCB7F9BA67C025EC3C5B3FED386E745E77DDD75D5A9E693B881F24
Malicious:	false
Reputation:	unknown
Preview:	KLIZU`.No.....\._...g....k'M.n.t....."(_.\<.F.&... .%xMW&DB...s.....GD.|...7..[.Oz.Q.m..P+...( D..7..F.nD=...t..X...w...p9~1...$u.X/..ze.....5P.&..n;.]n.o...W..ca....F...Z\.. ..u.8m...vs.i..y`.HP.|e.i..5..q...3"......9.b../...i.@..]..?.:ZH..w1...lQW.uW....x..8.Kmb+`M.lJ}..L....dq.....E....r..p0.....vt.=z9.....:...b....5.v..U'...8...z...Qg...+.x.X..]...?....h....p.."ZA. ..%\.....@.kd....."8..w;....."...>.}q....r.s.....y.{.....ps.n.6`...X*..Y.d.....x...;.]...71w...e=\....^.|TO..u..!.&3..'....~....:E.,q..I.....M..d?....."^..0..7.....O.T.....w9lH..F.....E2.f.i ....q...@....0-C|..*....q..*.....h....N.....<...../-..]..u..oU.Dm.UTr ..h...y..GS...5.F..'.w....K.F....(.e7.C...+....A..y.X.oxde?.k+...].$E...|.7..x:a..H....{..3Q.Z.."?F.@...V.WyY4y"Ca 3.|.\...)./.E[...q.(J...<h..C.."".....o...C.E.,...68...kZ...G..."..q!.X.,lJ.QZ..i..Y....s..|.....;M.....86o-j.)S..%9...Jx.....am...|....<.%..X.V....?..o/Klt.M.

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.843706691982694
Encrypted:	false
SSDEEP:	24:bMM+pr6jqg0JJxXc+bYHBBiOmHEB7NMPnk+ThgJy0/6niIPDbK4UzbFRMbD:p4kqg0JvceYHviO9+TSl/WiIPi4kID
MD5:	E48313B62F0FFA8D166E313D1508E3FB
SHA1:	6BF900328C7CE54CAFFCC6C90C6FDA33CBCAE594
SHA-256:	6918E86999BBC902192C83A6FC91D5E43233B1E1330DE3E3BF123A0C9F47A173
SHA-512:	7D403D47969F8ACF2CA8F06E39B1A6BADF06A58EBA3ADB0E69BCC82D3AD9666B10809A808ACCB7F9BA67C025EC3C5B3FED386E745E77DDD75D5A9E693B881F24
Malicious:	false
Reputation:	unknown
Preview:	KLIZU`.No.....\._...g....k'M.n.t....."(_.\<.F.&... .%xMW&DB...s.....GD.|...7..[.Oz.Q.m..P+...( D..7..F.nD=...t..X...w...p9~1...$u.X/..ze.....5P.&..n;.]n.o...W..ca....F...Z\.. ..u.8m...vs.i..y`.HP.|e.i..5..q...3"......9.b../...i.@..]..?.:ZH..w1...lQW.uW....x..8.Kmb+`M.lJ}..L....dq.....E....r..p0.....vt.=z9.....:...b....5.v..U'...8...z...Qg...+.x.X..]...?....h....p.."ZA. ..%\.....@.kd....."8..w;....."...>.}q....r.s.....y.{.....ps.n.6`...X*..Y.d.....x...;.]...71w...e=\....^.|TO..u..!.&3..'....~....:E.,q..I.....M..d?....."^..0..7.....O.T.....w9lH..F.....E2.f.i ....q...@....0-C|..*....q..*.....h....N.....<...../-..]..u..oU.Dm.UTr ..h...y..GS...5.F..'.w....K.F....(.e7.C...+....A..y.X.oxde?.k+...].$E...|.7..x:a..H....{..3Q.Z.."?F.@...V.WyY4y"Ca 3.|.\...)./.E[...q.(J...<h..C.."".....o...C.E.,...68...kZ...G..."..q!.X.,lJ.QZ..i..Y....s..|.....;M.....86o-j.)S..%9...Jx.....am...|....<.%..X.V....?..o/Klt.M.

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.841230712467715
Encrypted:	false
SSDEEP:	24:4Yp401V8dWwf1wSw2ItbfClLgqN7o64TWoCb3KOKX/xkfbD:4YpswwE22+lLsBTwVikDD
MD5:	991D453110F3E2DE9B9F66D5F4C91110
SHA1:	DD579C4142366C530F40F13EAC7CFC47F0A9A3D5
SHA-256:	7AFA7A0A874E9FC4EBA4E053CF89AE7F0A534BDE8D39FCA5BDF22F4F8E0DBB0D
SHA-512:	75CEDD0D44C2D670F0B29A3FD085D11FF36F24D186C80A512536A358DAFD0A6BB1AE8BB70B2DE96ED063819AAA91FD2271D8FC69CBC8657772D1FCBB0BB601E6
Malicious:	false
Reputation:	unknown

Preview:	NWCXB>.6..E....%...Z.G....!...c..#..G../0.y....mVM...Z..{u.).w.U._v....pw.K>}W|hpli1{...HJ.A(3zLB.r.>p....Z.0..|P.b"3#....=N...+....%...7.%\t...2nHn....c..e .[.7....C../..8..M/.._=f.. [G=..N. V..=.{o.<Pc... .....d$.}.+M....S.+....r..bd..Y../....5&m.....?"....jZ..5.cA,?"^...A.S)O.'-..e..J.....d.....C...s.z=G.:..=\|.$.Dv.. ... w_U.Q..p.1..+D(ehs...hJ..Tcdc.....w .#../.:3.}3..d."wY.....L.pn..-..1I.m....|.h...+O.....uU.X.n[..cgOA...!.VEL..#u..:.G.!l.,u...br.w..o.....d.....=o...8a...J..G..CH.JZ.D.c./...e8.....k.X1../..S.....-..E.....NGt..k'.....!...C [[.#LG.....F.....Q...N.7T.y-..RU.)..^.n..U..M.....!.D,....R.....vzo....X...`....1R...~.m..4..L$.e.K.O.`._.H(.....,}..J..&....7..Zj...*H ..ley..~..~.9.38....r....r;.c.F.?...>.....%}Y..l.. (.. \..I.4X.8..S....p..U.+..?..%l.ug.w.9.|=3.b.....rq{.2>...'d.]..<A.]3.....e.....6..[p6W.....9..|....Q..p.F.w.w..!.4.h..|K..Z|.H.;.[D.b..t..V/633...P..E..<4.0.]..w.}\x.P..L

C:\Users\user\Desktop\EIVQSAOTAQ\NWCXBPIUYI.jpg.vapo (copy)	
Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.841230712467715
Encrypted:	false
SSDEEP:	24:4Yp401V8dWwf1wSw2ltbfClLgqN7o64TWoCb3KOKX/xkfbD:4YpswwE22+lLsBTwVikDD
MD5:	991D453110F3E2DE9B9F66D5F4C91110
SHA1:	DD579C4142366C530F40F13EAC7CFC47F0A9A3D5
SHA-256:	7AFA7A0A874E9FC4EBA4E053CF89AE7F0A534BDE8D39FCA5BDF22F4F8E0DBB0D
SHA-512:	75CEDD0D44C2D670F0B29A3FD085D11FF36F24D186C80A512536A358DAFD0A6BB1AE8BB70B2DE96ED063819AAA91FD2271D8FC69CBC8657772D1FCBB0BB60 1E6
Malicious:	false
Reputation:	unknown
Preview:	NWCXB>.6..E....%...Z.G....!...c..#..G../0.y....mVM...Z..{u.).w.U._v....pw.K>}W|hpli1{...HJ.A(3zLB.r.>p....Z.0..|P.b"3#....=N...+....%...7.%\t...2nHn....c..e .[.7....C../..8..M/.._=f.. [G=..N. V..=.{o.<Pc... .....d$.}.+M....S.+....r..bd..Y../....5&m.....?"....jZ..5.cA,?"^...A.S)O.'-..e..J.....d.....C...s.z=G.:..=\|.$.Dv.. ... w_U.Q..p.1..+D(ehs...hJ..Tcdc.....w .#../.:3.}3..d."wY.....L.pn..-..1I.m....|.h...+O.....uU.X.n[..cgOA...!.VEL..#u..:.G.!l.,u...br.w..o.....d.....=o...8a...J..G..CH.JZ.D.c./...e8.....k.X1../..S.....-..E.....NGt..k'.....!...C [[.#LG.....F.....Q...N.7T.y-..RU.)..^.n..U..M.....!.D,....R.....vzo....X...`....1R...~.m..4..L$.e.K.O.`._.H(.....,}..J..&....7..Zj...*H ..ley..~..~.9.38....r....r;.c.F.?...>.....%}Y..l.. (.. \..I.4X.8..S....p..U.+..?..%l.ug.w.9.|=3.b.....rq{.2>...'d.]..<A.]3.....e.....6..[p6W.....9..|....Q..p.F.w.w..!.4.h..|K..Z|.H.;.[D.b..t..V/633...P..E..<4.0.]..w.}\x.P..L

C:\Users\user\Desktop\EIVQSAOTAQ\QCOILOQIKC.pdf	
Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.86283997564521
Encrypted:	false
SSDEEP:	24:wSd6jR55eH1UodzIYtOWp/ql76Las52dNdcMsVvAH2eAeKK1ob3c/eoMFtPbD:wS8jf5U1UoJIYb/ql76zkNiMiKMXKjJQ
MD5:	E7F90481213B679E3BFD9FB359B8C1BF
SHA1:	A72EB19239420D8D2219124AF73F03190DE7B3A2
SHA-256:	B46FC9B5AD0FBAC990D2E02C6A357C2FBFFEA7FA7F36E076306FB042CF8FB06F
SHA-512:	100AA68567551AA3F349B6B56EED9F154932970E94E46FF688FFE65E3717063B9053185FABD4DF49D07BF8EE1E71A58D684CFA93C7C81B14520238D8E38EE70E
Malicious:	false
Reputation:	unknown
Preview:	QCOIL...0_Q;..c..|.cj]K....&.'Q.YY6B.V.. M.R....RZ........_.KG..5...).&...21..3=...^,.QGL.. WL~.z..d..}S.C.. v..h\'9P...l...m..fx..a.-7.-Z..xY.....v....#.NE<R=.....Ps....m..dV.G.k. .@G>..e.\.>. ..FY._.2.yl.Q..l.....Ir..~.&h...P.^.U.>w.....< ..k_9.A...0...a5jk..S{...[.].!.....UL.8.7.....8.V#<e.....@..9..[.....O?0VP.....a...0..l5.....w.*..."#~f.B.T?.r_..Eu. ..K..$...\|r....0r..?T.....l..G-..@^...6.....X.yc..e.>z.X.....R.`/.PE.$..V...Y.O$$...I...<.4C...!.0.u.c....v..*;..rmg.....j..Nq".....E|.*...}.&.Bk.v...{...A.8..E4...q..S..>.'...*=x.@..#.7"....., P.G.....f9.6(.....2..Y.J....qK-.../.....wg[f7.!...?..i.....?\VfL...^..]k..Y...d...U....7.....$.....:..^kO...(.30..R..U..)q.S.I@4.A..i.u..@=.V,..@eys.;vG;.4..2...;jV.bT..y.....H.O.n.G. .....z(D{.a.....`h.....0..W./.L.+..(?.oW.....m\~.].....I.0.|..).p.bh.`.G*C.....a.Z....*%|....7`.v.....(..|y..<f.....<E*.(&.u.....N&..\.0..Z..fx].M...!wo.kL..c.....h.&...u.&

C:\Users\user\Desktop\EIVQSAOTAQ\QCOILOQIKC.pdf.vapo (copy)	
Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.86283997564521
Encrypted:	false
SSDEEP:	24:wSd6jR55eH1UodzIYtOWp/ql76Las52dNdcMsVvAH2eAeKK1ob3c/eoMFtPbD:wS8jf5U1UoJIYb/ql76zkNiMiKMXKjJQ
MD5:	E7F90481213B679E3BFD9FB359B8C1BF
SHA1:	A72EB19239420D8D2219124AF73F03190DE7B3A2
SHA-256:	B46FC9B5AD0FBAC990D2E02C6A357C2FBFFEA7FA7F36E076306FB042CF8FB06F
SHA-512:	100AA68567551AA3F349B6B56EED9F154932970E94E46FF688FFE65E3717063B9053185FABD4DF49D07BF8EE1E71A58D684CFA93C7C81B14520238D8E38EE70E
Malicious:	false
Reputation:	unknown

Preview:	QCOIL...0_Q;..c..|.cj]K....&.'Q.YY6B.V.. M.R....RZ....._.KG..5...).&...21..3=...^,.QGL.. WL~.z..d..}S.C.. v..h\'9P...l...m..fx..a.-7.-Z..xY.....v....#.NE<R=.....Ps....m..dV.G.k. .@G>..e.\.>. ..FY._.2.yI.Q..I.....Ir..~.&h...P.^.U.>w.....< ..k_9.A...0...a5jk..S{...[.].!.........UL.8.7.....8.V#<e.....@..9..[.....O?0VP.....a...0..l5.....w.*..."#~f.B.T?.r_..Eu. ..K..$...|r....0r..?T.....I..G-..@^...6.....X.yc..e.>z.X.....R.`/.PE.$..V...Y.O$$...I...<.4C...!.0.u.c....v..*;..rmg.....j..Nq".....E|.*...}.&.Bk.v...{...A.8..E4...q..S..>.'...*=x.@..#.7"....., P.G.....f9.6(.....2..Y.J....qK-.../.....wg[f7.!...?..i.....?\VfL...^..]k..Y...d...U....7....$.....:..^kO...(.30..R..U..)q.S.I@4.A..i.u..@=.V,..@eys.;vG;.4..2...:jV.bT..y.....H.O.n.G. .....z(D{.a.....`h.....0..W./.L.+..(?.oW.....m\~.].....I.0.|..).p.bh.`.G*C.....a.Z....*%|....7`.v.....(..|y..<f.....<E*.(&.u.....N&..\.0..Z..fx].M...!wo.kL..c.....h.&...u.&

C:\Users\user\Desktop\EIVQSAOTAQ\UNKRLCVOHV.png

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.827598154507707
Encrypted:	false
SSDEEP:	24:XPQuyqVQ6OKvTDCN6HjF8SGSIqcpEH5TXM5n3WfygykMPyGqxmJbD:XPQLqVTOSjF81Sziu5TM53+I7QmpD
MD5:	AC9B11EDFCA0CD185E8C5D51A49ED6CC
SHA1:	8F46FEA35BF3A65864D2F3FDB9EF882F12F1D905
SHA-256:	7F2C2EA60BD6FA85F986FD8CDC4E6530FAE429FEB3991E6E71036BC1664EBE19
SHA-512:	A918E103ACE91C94FADD754D61EA81206DE53C5C4A9523B8D4B33DD650C311A08BFFEFD28F2DA35428E2612F50CB0308A5655BE1BF6E33432AA16228A26252 A
Malicious:	false
Reputation:	unknown
Preview:	UNKRLP.@>..P.0.`z..v...w!.....c:.Jy.x......e...\..e?%?..E...v.6.f.~U_..v..o&"3..._...F+p%@.~....i.....4E8.w6JE..w.u..^@A.;cz.....S...G...g.....0..)r~.[...s.>..P.+....?...g.<;(C;..Z ...7..W.p.8..V..E.izo...........AD.8..%..e,..Z..:.`.s....s..(...IE...".q4.a/.N....nh.....a....R.+.:.....k.....; ..j.i..>...K.,vZ....@EVL...k.....'i.....QA..-.....U.T..W...o...I.w74n.XD@.B.8.~..x .rZk..-.x.....7..77..P\...&..\a..i.....8!...}.....1qqM.j...........A.t".....Cp.@...O.....P..p..E.5.>..O..a.j.m.c3.6_..G..Ksv@.-....M.D..-P.....P[.....ZcX.pX.$.w7...i.d.1...}7|t...L:..... vz/..Jw.l.3.....m..k.....W4..r...;d}.....<..#.9..].&>..i.hb..N.l..4me...VU.....5'.Q.].....S'.\...BKq....<.2.^..Z55o.>*n.....[...^L...G_.b.....e.W..#*VR5..l..3.S.Y.[.y..W9...W.F-p0..1..I .#.^.]G...4..RL..T...jZ..#..O;.G\...)KI0..V....Q....6...-Gu...:.6'hWO.=\."........T6A..^.....7....QHh.H....%.nLk/K.Pq..1g.....e..N:..#]...7F...'4...BH.....>!.A

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.827598154507707
Encrypted:	false
SSDEEP:	24:XPQuyqVQ6OKvTDCN6HjF8SGSIqcpEH5TXM5n3WfygykMPyGqxmJbD:XPQLqVTOSjF81Sziu5TM53+I7QmpD
MD5:	AC9B11EDFCA0CD185E8C5D51A49ED6CC
SHA1:	8F46FEA35BF3A65864D2F3FDB9EF882F12F1D905
SHA-256:	7F2C2EA60BD6FA85F986FD8CDC4E6530FAE429FEB3991E6E71036BC1664EBE19
SHA-512:	A918E103ACE91C94FADD754D61EA81206DE53C5C4A9523B8D4B33DD650C311A08BFFEFD28F2DA35428E2612F50CB0308A5655BE1BF6E33432AA16228A26252 A
Malicious:	false
Reputation:	unknown
Preview:	UNKRLP.@>..P.0.`z..v...w!.....c:.Jy.x......e...\..e?%?..E...v.6.f.~U_..v..o&"3..._...F+p%@.~....i.....4E8.w6JE..w.u..^@A.;cz.....S...G...g.....0..)r~.[...s.>..P.+....?...g.<;(C;..Z ...7..W.p.8..V..E.izo...........AD.8..%..e,..Z..:.`.s....s..(...IE...".q4.a/.N....nh.....a....R.+.:.....k.....; ..j.i..>...K.,vZ....@EVL...k.....'i.....QA..-.....U.T..W...o...I.w74n.XD@.B.8.~..x .rZk..-.x.....7..77..P\...&..\a..i.....8!...}.....1qqM.j...........A.t".....Cp.@...O.....P..p..E.5.>..O..a.j.m.c3.6_..G..Ksv@.-....M.D..-P.....P[.....ZcX.pX.$.w7...i.d.1...}7|t...L:..... vz/..Jw.l.3.....m..k.....W4..r...;d}.....<..#.9..].&>..i.hb..N.l..4me...VU.....5'.Q.].....S'.\...BKq....<.2.^..Z55o.>*n.....[...^L...G_.b.....e.W..#*VR5..l..3.S.Y.[.y..W9...W.F-p0..1..I .#.^.]G...4..RL..T...jZ..#..O;.G\...)KI0..V....Q....6...-Gu...:.6'hWO.=\."........T6A..^.....7....QHh.H....%.nLk/K.Pq..1g.....e..N:..#]...7F...'4...BH.....>!.A

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.842576313328374
Encrypted:	false
SSDEEP:	24:Rwf2ADFGoTP12WNodekkgFwF4veDqAsRFKZIuRqthtA7UjNmRbD:efRGoNNoPkLZOAnytj0WNmBD
MD5:	65D8518DAE026062A4DC98ADCE837228
SHA1:	3AB538370E5DABC760416225CF88983A37BABF6D
SHA-256:	F3AD98BD36A5B1BFF39A4A0028C8DDA5A7A5AC7C151C37A36A044A2D07074B41
SHA-512:	77D9A766FBD23ABEAE364D1D1B2EF13689AAB2BCAD7C040676DE6293C92CE958C039EA6263ED2BD351145AE065FD3C955A29F6D4CFCF004D71A240A8C51A7 756
Malicious:	false
Reputation:	unknown

Preview:	EOWRV.... ..C.J..Y..s.(.i...o.Nu".]pX....b6..u...6>7{`..DZ....@X....DM..l.dn..O7.}.G.SOg`.9...I..atn...u.'d..I..M....M.!.6.5.Z&....F...;Z;.2.j.KV.[=.f..c.b.s.>y&E2..m....X....3b.C/ X..t....yA.....m..._.... .P.)0q.>{.i ...v..\...]v.....G.CX.5....._.s.>..K.GPO...?....UJ=....L~.....xh..r....n.?.w...V?d-.....6d:.*.....M.b..M..jl.Sh`.G....C...q.,0 .).2.P.....o.....!..Q+~. .b.'.l.?I..3.BG0...E>...+.....(..2R..[...].....b..\.%..w.|z..U.D.....f...lJw...;.....xt...zV...D.t..<..>..F.i.bD.....@..@.....YE*.B]%....=..v....H...x.....TA.y. ....e,uUQ.e...W.....P.li. .5....}VV..A..8Vq.....Kb...F..s]j.....&.....;...Dl).S..q..D.<.'....=x.p.....+v..!....|pCP.x8...0k....F.mG.....M.=..WK.....e.JU.s.L...z[.2Q...W-.awre.<C..].....H{*.7.".j.@.Q`.."... @.z.....=.Ik...N.n.....E.?I...]..o.....g..k(.".W.oR..../.L.EK...q:/W..E.....nr...-7.>L....@+.....#2.....|G.U`.....r.....r.....g.....6.....*C.../"./.f.j..=..j>H*...

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.842576313328374
Encrypted:	false
SSDEEP:	24:Rwf2ADFGoTP12WNodekkgFwF4veDqAsRFKZluRqthtA7UjNmRbD:efRGoNNoPkLZOAnytj0WNmBD
MD5:	65D8518DAE026062A4DC98ADCE837228
SHA1:	3AB538370E5DABC760416225CF88983A37BABF6D
SHA-256:	F3AD98BD36A5B1BFF39A4A0028C8DDA5A7A5AC7C151C37A36A044A2D07074B41
SHA-512:	77D9A766FBD23ABEAE364D1D1B2EF13689AAB2BCAD7C040676DE6293C92CE958C039EA6263ED2BD351145AE065FD3C955A29F6D4CFCF004D71A240A8C51A7 756
Malicious:	false
Reputation:	unknown
Preview:	EOWRV.... ..C.J..Y..s.(.i...o.Nu".]pX....b6..u...6>7{`..DZ....@X....DM..l.dn..O7.}.G.SOg`.9...I..atn...u.'d..I..M....M.!.6.5.Z&....F...;Z;.2.j.KV.[=.f..c.b.s.>y&E2..m....X....3b.C/ X..t....yA.....m..._.... .P.)0q.>{.i ...v..\...]v.....G.CX.5....._.s.>..K.GPO...?....UJ=....L~.....xh..r....n.?.w...V?d-.....6d:.*.....M.b..M..jl.Sh`.G....C...q.,0 .).2.P.....o.....!..Q+~. .b.'.l.?I..3.BG0...E>...+.....(..2R..[...].....b..\.%..w.|z..U.D.....f...lJw...;.....xt...zV...D.t..<..>..F.i.bD.....@..@.....YE*.B]%....=..v....H...x.....TA.y. ....e,uUQ.e...W.....P.li. .5....}VV..A..8Vq.....Kb...F..s]j.....&.....;...Dl).S..q..D.<.'....=x.p.....+v..!....|pCP.x8...0k....F.mG.....M.=..WK.....e.JU.s.L...z[.2Q...W-.awre.<C..].....H{*.7.".j.@.Q`.."... @.z.....=.Ik...N.n.....E.?I...]..o.....g..k(.".W.oR..../.L.EK...q:/W..E.....nr...-7.>L....@+.....#2.....|G.U`.....r.....r.....g.....6.....*C.../"./.f.j..=..j>H*...

C:\Users\user\Desktop\EOWRVPQCCS\EIVQSAOTAQ.pdf

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.854672599982638
Encrypted:	false
SSDEEP:	24:R2Al2ID+qDSG5SkBxG5583fzZwNL4E4e7OrffvTK47DE/mOA5AieGTM3IbD:3l2FCSGskJzIJ7O7vTZs/m/57TM3SD
MD5:	6A1AC5F901C5A8E124678C648D52210C
SHA1:	F6E2081E178B1CA55D4625DEDE668C34AE51E034
SHA-256:	70B77C6B2E368B2411EDB547C2128D0257CAA00FE830EEEEF543967AA7D56ABF
SHA-512:	0379272E23D4811CCFCAD7F0CDFB2E691080FA8A436005D8189CBBCE480B6CC8F7CA0E9876ED41F7243EE9E10EA48DD8CF99D42D47B7916431BBFA61D04C2 7D
Malicious:	false
Reputation:	unknown
Preview:	EIVQS...C.....E)......'.i=^........P.xf..$.7..m.EXu\|...3.i.V..&x.J....L...rK.....%PW.@../..EM>W.:.Y=V...9R.fy\|.<=,....k..)...h.1....q...i.P3h.f.....;;"....R.!...2..UU..c2.....sR"eg....W)!.9... .;..k.&Y.$*..X... ......).kc"W/L.....$.a..?..dH.,.9..A.c...*d.EN0..`.E.....k..._....#...FP.RU...Y...$..5...TW..a_..h..;....~-].vD}....!}.cc..-9..;M.[.....x....F..f.....>.....1.WD.ct.Y.^+ .....0~..=!....u~I.<@.rs.....;...K.z..q.J.mt.M"X).5Tbd.....vj..!..1N....b.L.`.#....."..wt3T..9|r..L.?.w#046....ElfYn.w8.{_.>&....t.....7.I8Q..o.;R.U.....1.L....kL .K.1...=..<c..1h.C..! [F)p...'qsp.ha9W...)UQ/.k.V....w.:W.....3.=.kF....;oc..=..t.@U.w.....I.....y..u?...R.!.Q...s.on...z./.5..+|....J..Uq....7.....g...}5..y.....p.l~..8.y.<....p..P.....M";.m.]G. ..o.87.>Qc.J.O^t..#..|.emu...4Vmf..z....e.X/`.-x.....dXl.tY7e.....i."6.e...m.....TRO]43`.%.=[....C..x.?..IZ..?.....].EQ...N....u-t.{..8>\.....w.J...U|c.PwCk6..,`..

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.854672599982638
Encrypted:	false
SSDEEP:	24:R2Al2ID+qDSG5SkBxG5583fzZwNL4E4e7OrffvTK47DE/mOA5AieGTM3IbD:3l2FCSGskJzIJ7O7vTZs/m/57TM3SD
MD5:	6A1AC5F901C5A8E124678C648D52210C
SHA1:	F6E2081E178B1CA55D4625DEDE668C34AE51E034
SHA-256:	70B77C6B2E368B2411EDB547C2128D0257CAA00FE830EEEEF543967AA7D56ABF
SHA-512:	0379272E23D4811CCFCAD7F0CDFB2E691080FA8A436005D8189CBBCE480B6CC8F7CA0E9876ED41F7243EE9E10EA48DD8CF99D42D47B7916431BBFA61D04C2 7D
Malicious:	false
Reputation:	unknown

Preview:	EIVQS...C.....E).....'.i=^.....P.xf..$.7..m.EXu\|...3.i.V..&x.J....L...rK.....%PW.@../..EM>W.:.Y=V...9R.fy\|.<=,....k..)...h.1....q...i.P3h.f.....;;"....R.!...2..UU..c2.....sR"eg....W)!.9...-.;..k.&Y.$*..X... .....).kc"W/L.....$.a..?..dH.,.9..A.c...*d.EN0..`.E.....k.._....#...FP.RU...Y...$..5...TW..a_..h..;....~.].vD}....!}.cc..-9..;M.[.....x....F..f.....>.....1.WD.ct.Y.^+.....0~..=!....u~I.<@.rs.....;...K.z..q.J.mt.M"X).5Tbd.....vj..!..1N....b.L.`.#....."..wt3T..9|r..L.?.w#046....ElfYn.w8.{_.>&....t.....7.I8Q..o.;R.U.....1.L....kL .K.1...=..<c..1h.C..![F)p...'qsp.ha9W...)UQ/.k.V....w.:W.....3.=.kF....;oc..=..t.@U.w.....I.....y..u?...R.!.Q...s.on...z./.5..+|....J..Uq....7.....g...}5..y.....p.I~..8.y.<....p..P.....M";.m.]G...o.87.>Qc.J.O^t..#..|.emu...4Vmf..z....e.X/`.-x.....dXl.tY7e.....i."6.e...m.....TRO]43`.%.=[....C..x.?..IZ..?.....].EQ...N....u-t.{..8>\.....w.J...U|c.PwCk6..,`..

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.847178803856652
Encrypted:	false
SSDEEP:	24:NzqVMQEL4MvCfoSe6moSKOsc+hDV0l4eX5tE39uTltib4tXpzA1ibCl2gA91fxVX:p6MQk4nfoD6mR4hD+xIXIBta41kFD
MD5:	B1A4DE06C1897E7B91FE0437AF0248FB
SHA1:	174AE49EE8A52687462233FB8338B0A6E6F92E25
SHA-256:	4CD70D01A220561F53C322E7EB5F6C99D33A8D890B58A26C0FCFBAFDA8F5D7F5
SHA-512:	F8A503BA751B267808B20EF8753830BF72A46D394D8EE0020CD43F783DAD2F6A1E7F6CA07A3084084333834620CF80B49D0D6D734E8192C5F0988AFBEA3A2F0(
Malicious:	false
Reputation:	unknown
Preview:	EOWRV;k.w@a..6..M3@..e.'K@.$.rtn.:.6..X.\|....r...M.'eh..o[H.~.X.NH.....E...sH[P.&3..'..".4f]...\|O.k.?...[.%.....3.z2.b.K.../{.F.r..m.~.TM.....g.Y......R=n.. .`s2f..]....;*cj..}..bu..g.b.[.?M../_y."o..a.....,2' G.H_..A.....XY.Q`..a= ..k/0..Wf...Xs..Pt.....%.F.E.?....Q.ry[.....X.8i..q....>..~aPG.^.b&H...*..[..B..J m. .....U..#/3.8....'9=...;.c7...g..>....Yi-...+.C.....`.t.,{E..YAH.7.3..B:...}...R.Q...f.n.F...2(..+..0..0..@vY.....j....I?..\Q.(..;...-H.7.O_'_...A.W...zixeU..@.....6..1-.....TC..v.'A.8O...5....x.)Q`6f..4..n.D..+.mn..#... ~.i.li.C..!.(.>,j2..Pt..N.)....C.U.....N=.K3.a.....R..:.....3.'.wHX.7...:J.J....W.....G8..y...X.....r.....j....[.!.gh\.Zm.<Q.r.BE.:_.....Q...j...X.$.[.....k.R.i`.....I.a-D.0.\LJ....."G..R....*X..Uf...7I.@.8k&.s.<Kj..5...4.R).E.:...;,....3F...L....>.@.jf $0....>.....{....$].L..`....w..|.....O....n..7<....._.G~.E."./!O;/....3.X.p..mtw<l:j.O`|Z.#..O.M..F.).{..l..+...29N.U...b.%

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.847178803856652
Encrypted:	false
SSDEEP:	24:NzqVMQEL4MvCfoSe6moSKOsc+hDV0l4eX5tE39uTltib4tXpzA1ibCl2gA91fxVX:p6MQk4nfoD6mR4hD+xIXIBta41kFD
MD5:	B1A4DE06C1897E7B91FE0437AF0248FB
SHA1:	174AE49EE8A52687462233FB8338B0A6E6F92E25
SHA-256:	4CD70D01A220561F53C322E7EB5F6C99D33A8D890B58A26C0FCFBAFDA8F5D7F5
SHA-512:	F8A503BA751B267808B20EF8753830BF72A46D394D8EE0020CD43F783DAD2F6A1E7F6CA07A3084084333834620CF80B49D0D6D734E8192C5F0988AFBEA3A2F0(
Malicious:	false
Reputation:	unknown
Preview:	EOWRV;k.w@a..6..M3@..e.'K@.$.rtn.:.6..X.\|....r...M.'eh..o[H.~.X.NH.....E...sH[P.&3..'..".4f]...\|O.k.?...[.%.....3.z2.b.K.../{.F.r..m.~.TM.....g.Y......R=n.. .`s2f..]....;*cj..}..bu..g.b.[.?M../_y."o..a.....,2' G.H_..A.....XY.Q`..a= ..k/0..Wf...Xs..Pt.....%.F.E.?....Q.ry[.....X.8i..q....>..~aPG.^.b&H...*..[..B..J m. .....U..#/3.8....'9=...;.c7...g..>....Yi-...+.C.....`.t.,{E..YAH.7.3..B:...}...R.Q...f.n.F...2(..+..0..0..@vY.....j....I?..\Q.(..;...-H.7.O_'_...A.W...zixeU..@.....6..1-.....TC..v.'A.8O...5....x.)Q`6f..4..n.D..+.mn..#... ~.i.li.C..!.(.>,j2..Pt..N.)....C.U.....N=.K3.a.....R..:.....3.'.wHX.7...:J.J....W.....G8..y...X.....r.....j....[.!.gh\.Zm.<Q.r.BE.:_.....Q...j...X.$.[.....k.R.i`.....I.a-D.0.\LJ....."G..R....*X..Uf...7I.@.8k&.s.<Kj..5...4.R).E.:...;,....3F...L....>.@.jf $0....>.....{....$].L..`....w..|.....O....n..7<....._.G~.E."./!O;/....3.X.p..mtw<l:j.O`|Z.#..O.M..F.).{..l..+...29N.U...b.%

C:\Users\user\Desktop\EOWRVPQCCS\EWZCVGNOWT.jpg

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.858964908680031
Encrypted:	false
SSDEEP:	24:jEzfqvuPk6Hu05Whq1rlOk334wAd1UXH5WUnv3p8YpnEgqkuRTWVh5Jek+6fbD:jMz86OcWeI5j5WUnv3pHEpNTWVh5JeTk
MD5:	CD24CA4CB06A00BE1442D3BB7D1885A3
SHA1:	66EAC12DD4FAED7F2C2E886283DBC855DBFF58AB
SHA-256:	7A5EEDC4DD9BFC12BFCED58BD96EF9C0EF29F431771200CD8626F9D690021DAC
SHA-512:	76F95BA7F1EB3E16BA8547EE4B29C02334228B09392463133DA5ECA58E9EDEECC4E3AAAD3409807BD1EF8F8DE1AF8E695F5F01E5340929AE292D7ECCD31AAA97
Malicious:	false
Reputation:	unknown

Preview:	EWZCV..x.>..P.H...E....#,gya.`:fo..'1J.d..z.....*e$L.....Qs}..kD.@.3r}.j.....?.c<.\[..%C.b..;.-DGN....~.F8...b.....vNV<x...g.#.2C.z.t[{>.]IJ..\...z_.V.x...6{.]8...&p[.g.c..F.....x....C.... .?3..;!..+...)....: j!n..S.-...U(.J.t.yh.}.....!...5"...+.H..+.HYY.....a..FkY`L.`.....&w.+s..j.%m..`...V....(.....F.....?kmnB$+ ..P..M.....27...S...}._..$=...7:%'}...=.m2&.-.k*Qs.x.... .....Z.0.....6?.....x.^.,.#S_E.o..Z....3...b....G+o..5[...M...}..#w..`..C.$..o.{`..x.....}.....J..r...c....q....c..B=.5gv.S...1.L.....?H3.....y..e.FS..@....CNL].HF>..o..I.2.....EG....\}... }.=.....T.....&..6./.....L.2.....*.. W..b_..f..C(.....e...v..'...A.m...o7....FX.....l]....X.y.y..cTC.I...(...*..A....O..@.....Q4x.o...\7ll*.e...K.....rF.YM.56gQ....._P.3.5uI*$...)i..._E..|#h 5/....S..F(.6....!....?g..A...}.ea....y.(k.c|.....m.M...*1E...$...69....zm... %D..("....O....h.....->d.`TB..3.....wD.<T....a..}.....^I..D.....e.}

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.858964908680031
Encrypted:	false
SSDEEP:	24:jEzfqvuPk6Hu05Whq1rIOk334wAd1UXH5WUnv3p8YpnEgqkuRTWVh5Jek+6fbD:jMz86OcWeI5j5WUnv3pHEpNTWVh5JeTk
MD5:	CD24CA4CB06A00BE1442D3BB7D1885A3
SHA1:	66EAC12DD4FAED7F2C2E886283DBC855DBFF58AB
SHA-256:	7A5EEDC4DD9BFC12BFCED58BD96EF9C0EF29F431771200CD8626F9D690021DAC
SHA-512:	76F95BA7F1EB3E16BA8547EE4B29C02334228B09392463133DA5ECA58E9EDEECC4E3AAAD3409807BD1EF8F8DE1AF8E695F5F01E5340929AE292D7ECCD31AAA97
Malicious:	false
Reputation:	unknown
Preview:	EWZCV..x.>..P.H...E....#,gya.`:fo..'1J.d..z.....*e$L.....Qs}..kD.@.3r}.j.....?.c<.\[..%C.b..;.-DGN....~.F8...b.....vNV<x...g.#.2C.z.t[{>.]IJ..\...z_.V.x...6{.]8...&p[.g.c..F.....x....C.... .?3..;!..+...)....: j!n..S.-...U(.J.t.yh.}.....!...5"...+.H..+.HYY.....a..FkY`L.`.....&w.+s..j.%m..`...V....(.....F.....?kmnB$+ ..P..M.....27...S...}._..$=...7:%'}...=.m2&.-.k*Qs.x.... .....Z.0.....6?.....x.^.,.#S_E.o..Z....3...b....G+o..5[...M...}..#w..`..C.$..o.{`..x.....}.....J..r...c....q....c..B=.5gv.S...1.L.....?H3.....y..e.FS..@....CNL].HF>..o..I.2.....EG....\}... }.=.....T.....&..6./.....L.2.....*.. W..b_..f..C(.....e...v..'...A.m...o7....FX.....l]....X.y.y..cTC.I...(...*..A....O..@.....Q4x.o...\7ll*.e...K.....rF.YM.56gQ....._P.3.5uI*$...)i..._E..|#h 5/....S..F(.6....!....?g..A...}.ea....y.(k.c|.....m.M...*1E...$...69....zm... %D..("....O....h.....->d.`TB..3.....wD.<T....a..}.....^I..D.....e.}

C:\Users\user\Desktop\EOWRVPQCCS\GIGIYTFFYT.png

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.835024831052557
Encrypted:	false
SSDEEP:	24:EXomp4C/wx+FrCK0dHemvaRiFeN5xZviR0b97ib/3j38PnIguJFbD:tagHeWFcmR0pebQnIlD
MD5:	7F57B1DDDD4684DCD34912C2BB7E4A7A
SHA1:	5D0B211133C8593FAE0FCE538ABC99C4EBBE605C
SHA-256:	7CA04A5820649EB8DE6A1B517D3C7A83A29088BE17F2F208CBAA475E56F4B453
SHA-512:	6D11F1FAB3A46EC351142EE2399FE4560B00F4988F20B820F1629DE3C1656F81A22D023AFAFE34A119D6F033D3627578E3DF9EA01505E9E233B50556EC884FA3
Malicious:	false
Reputation:	unknown
Preview:	GIGIY%..P:..?./.uk.`...?4..R..c.A..q."LuG...G....7Ew....HC..E(.Hu..u..W.g..CP..&ILB..E.....ACa.g.5....G...p.Eh.,..~...}.HFy.rT...jk."G...c.. ...a.[...,.U@..s/,Q.s8.....=....y..&M.. ^P.....@..Z....?.*.FY..&.,....t<=1.....g^G.~.....h...2.G)A1^.A.z....,....].dw.{.....,!.\. &(...#.._N...Y.X`...g.@..!.....2....j..kH.p.)V.....e....i..3h.\.9..JRO.....f.....H.3..b..w.(W..~.\F. [\N.{..g....,]Kc..i...@UqVa.W....J$....D.....KM.&.5Gq.....a]&....,..c..q.....v(#.0|...m{.o./...MB.t.:.;...*E2.$.{..j.D?...?..v.Hlz.m8.... ..e.d..+.....T..$3I=.....+....${.....S.... %.....p.....P...d.../...5S`.sh...e..:..oC.....dJ35y.....&{.."......!.:g.R.....].,<.`....H$.#.....nNy|.....j.<`....j.je.~...H&..gUz.....5...z.9.W(D.1.Oh:...6OJ,.7..<...>.w.ho..'NV.t.....v(.... x..&...#x..9=..b..m.q.I&.~.0%OO. $.....VxM.....r.x..`6JH....j.+g...$...../..z...@.U]..D.o...a.O...hpE.t...6.Y..L.d.....g7.../..&%@u..D.U>e.W.....v....5.j-..'..a=..9.

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.835024831052557
Encrypted:	false
SSDEEP:	24:EXomp4C/wx+FrCK0dHemvaRiFeN5xZviR0b97ib/3j38PnIguJFbD:tagHeWFcmR0pebQnIlD
MD5:	7F57B1DDDD4684DCD34912C2BB7E4A7A
SHA1:	5D0B211133C8593FAE0FCE538ABC99C4EBBE605C
SHA-256:	7CA04A5820649EB8DE6A1B517D3C7A83A29088BE17F2F208CBAA475E56F4B453
SHA-512:	6D11F1FAB3A46EC351142EE2399FE4560B00F4988F20B820F1629DE3C1656F81A22D023AFAFE34A119D6F033D3627578E3DF9EA01505E9E233B50556EC884FA3
Malicious:	false
Reputation:	unknown

Preview:	GIGIY%..P:..?./.uk.`...?4..R..c.A..q."LuG...G....7Ew....HC..E(.Hu..u..W.g..CP..&lLB..E.....ACa.g.5....G...p.Eh.,..~...}.HFy.rT...jk."G...c.. ...a.[...,U@..s/,Q.s8.....=....y..&M.. ^P.....@..Z....?.*.FY..&.,....t<=1.........g^G.~.....h...2.G)A1^.A.z....,....].dw.{.....,!.\. &(...#._N...Y.X`...g.@..!.....2....j..kH.p.)V.....e....i..3h.\.9..JRO....f.........H.3..b..w.(W..~.\F. [\N.{..g....,]Kc..i...@UqVa.W....J$.....D.....KM.&.5Gq.....a]&....,..c..q.........v(#.0|...m{.o./...MB.t.:.;...*E2.$.{..j.D?...?..v.Hlz.m8.... ..e.d..+.....T..$3I=.....+....${.........S.... %.....p.....P...d.../...5S`.sh...e..:..oC.....dJ35y.....&{..".....!.:g.R.........].,<.`....H$.#.....nNy|.....j.<`....j.je.~...H&..gUz.....5...z.9.W(D.1.Oh:...6OJ,.7..<...>.w.ho..'NV.t.....v(.... x..&...#x..9=..b..m.q.I&.~.0%OO. $.....VxM.....r.x..`6JH....j.+g...$...../..z...@.U]..D.o...a.O...hpE.t...6.Y..L.d.....g7.../..&%@u..D.U>e.W.....v...5.j-..'..a=..9.

C:\Users\user\Desktop\EOWRVPQCCS\KLIZUSIQEN.mp3

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.816943134843193
Encrypted:	false
SSDEEP:	24:bjNe2RCZqKadY/MESG+A1DgUjMsjlPruGEu6MFYFWa53fmF5VldkaRBkm5+bD:fM2RCQvdSSBA1MAMsjlDrHFYFd+R7RBS
MD5:	29312249CC623973AF0003CDAC960977
SHA1:	7BE3FA6911887CFE816431830E2259006740BAB0
SHA-256:	7CA708B01B1391456219C0614A015BA4A5B5976784C1B8C10F739D0C73302D6D
SHA-512:	410022D768AFFB22D64DB542154F6542CA1037A2EF146B13AF749A9C3A3432A036C8869110C38601F7B439CC5A007C7B5CADB08D61C1F5779AE8534955C8F7E4
Malicious:	false
Reputation:	unknown
Preview:	KLIZU.....k....{.P L.K.1..P.....Z.Kot..$FD.+.B.~.6....AX]-..<.G.x/...8....!Fm.....b.2^x;e...%j.*.....-`..r.....d.#".v.t....@U.....t....._.&h....t[.p#T2..\O.{.....I.]SB.\.0.k...K.p\... xB..RT..K}....AF.....[M.....q...zrX%...Z..O...'rJ..n...?.....e.(..P.....1.P.....gO....|..`...]<l.....[.d19B.G.....8.<.>.u.....5Y .....-....F.Y...X|.B.....f.Pk...T.(;yR.....Z..@W.H..P. [.;...".....,'.>.:_Et..`=.w.h..n.....O..e...Cl...N.J+..|.....fr..I.X\)p..P.....W.....Z]\7....M....4..s.....2..../.~0.....j|dF.].....7.x..:.#..@.8.v.....2So...j#?.H.....A..:....Q{..u.WJ.....Py.r.A...m .2...?.M.~..VA.....}..O..h.|.9.....Z.(.A.9.P}G.C.,.....G1.&.C...D@...&.../....vk3.z#. {;.E....p...+..O.....>....x1...F..ih....)..\..awG...<..M.XN..Mn..0...g....:....A.9..;r13....<..q.7. ."...g\.....P|...Z....yk.-Sr.+o....7c.k,N.&@w...ti..q.6..`x._.....E.K.T..&..:.wh.h.L.@.|.~.,.^y.{.No..6...k..G.....90...~.H...X..\....?....b'+....

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.816943134843193
Encrypted:	false
SSDEEP:	24:bjNe2RCZqKadY/MESG+A1DgUjMsjlPruGEu6MFYFWa53fmF5VldkaRBkm5+bD:fM2RCQvdSSBA1MAMsjlDrHFYFd+R7RBS
MD5:	29312249CC623973AF0003CDAC960977
SHA1:	7BE3FA6911887CFE816431830E2259006740BAB0
SHA-256:	7CA708B01B1391456219C0614A015BA4A5B5976784C1B8C10F739D0C73302D6D
SHA-512:	410022D768AFFB22D64DB542154F6542CA1037A2EF146B13AF749A9C3A3432A036C8869110C38601F7B439CC5A007C7B5CADB08D61C1F5779AE8534955C8F7E4
Malicious:	false
Reputation:	unknown
Preview:	KLIZU.....k....{.P L.K.1..P.....Z.Kot..$FD.+.B.~.6....AX]-..<.G.x/...8....!Fm.....b.2^x;e...%j.*.....-`..r.....d.#".v.t....@U.....t....._.&h....t[.p#T2..\O.{.....I.]SB.\.0.k...K.p\... xB..RT..K}....AF.....[M.....q...zrX%...Z..O...'rJ..n...?.....e.(..P.....1.P.....gO....|..`...]<l.....[.d19B.G.....8.<.>.u.....5Y .....-....F.Y...X|.B.....f.Pk...T.(;yR.....Z..@W.H..P. [.;...".....,'.>.:_Et..`=.w.h..n.....O..e...Cl...N.J+..|.....fr..I.X\)p..P.....W.....Z]\7....M....4..s.....2..../.~0.....j|dF.].....7.x..:.#..@.8.v.....2So...j#?.H.....A..:....Q{..u.WJ.....Py.r.A...m .2...?.M.~..VA.....}..O..h.|.9.....Z.(.A.9.P}G.C.,.....G1.&.C...D@...&.../....vk3.z#. {;.E....p...+..O.....>....x1...F..ih....)..\..awG...<..M.XN..Mn..0...g....:....A.9..;r13....<..q.7. ."...g\.....P|...Z....yk.-Sr.+o....7c.k,N.&@w...ti..q.6..`x._.....E.K.T..&..:.wh.h.L.@.|.~.,.^y.{.No..6...k..G.....90...~.H...X..\....?....b'+....

C:\Users\user\Desktop\EOWRVPQCCS\ZGGKNSUKOP.xlsx

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.844251223691602
Encrypted:	false
SSDEEP:	24:4n/R54HotLcNcITUYyD/mWnzEL6VcN7dz8ondYP6YE6lUmFzD64qCtSP6MbD:4AHMIgJzvn4icNaE6gmFrq6SiGD
MD5:	6F195CDAB01B0D696CFEEC8DAE39C24B
SHA1:	4C021B1060F156AA0CF367BEEFACF97CE023266C
SHA-256:	FC81DD32E4E7FB2C1D1FFFCDCB8B3856DE18807EA6D585FF4C8366767CF43CE6
SHA-512:	F95BDC00338820478A54FE3BB9A4A929A7EB040120ACFAC891245C9C667F14BDFA45CA2C5306A3E688F3C79A391314528AAA7C88FAAE8F64E58ADB763AF62CA3
Malicious:	false
Reputation:	unknown

Preview:	ZGGKN.+.h.....'.D=...+/w>.XFt.....&|..'....o.....dY..z.~...i3y...5M...G..$.t.2.....kGG.I...hj...]EmJI....h....wP.Hi...9....=.=.@C:...\..2....p.....2]t..E...^.K...m..O..N..t..z ..u..WQ.y.o}+A..E.>.....~.Nf. _...T.c.....\|8..q.r1C.I...]..f....<..!.T.5..]....I.,.x@..O..gm.....fh@.hQ...U.L..X\...7A0.2..>e.5..`.'.M.....w.....O.....1.6H...."H{..l.1.px.x.5GFoU3... .y.'.....y<.*.T..S..xE.....t..@.Gl.z2.....W".G\|..}.....%..'7..:[.f.:W..m....p..\..1y....1....$..5H.!..Y9KP.R.1_...P%O==*.d.N.....c'..i{.J.-.k..iX...B.b%<\q.....N...|..L[[..(..5.^.y....yQ.'7..? =9..\....0....v.U.FKV,.-.MR.Q7..P.e.].....I.A.h..m...(.}(.K.....r4. .i...W.D.6.be.=.....g..t..d..)....i.....k+.fW.V.7.%.F...?.....q.+!=?.U..-U..... ..*.F..T.....LL..V.$.r...a9mC@.y...(.... f.wy(-..aF.g6u..n.tP...T5..`..j.....&.Z.].0.y..l.z.....[....8,.q.,....R.L.m...+'.Z..k..^.J(...b.1S.....?.4...J.....t...Q.....4j..j.x.....So.J.X..l.....<.....M..<n.

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.844251223691602
Encrypted:	false
SSDEEP:	24:4n/R54HotLcNclTUYyD/mWnzEL6VcN7dz8ondYP6YE6lUmFzD64qCtSP6MbD:4AHMlgJzvn4icNaE6gmFrq6SiGD
MD5:	6F195CDAB01B0D696CFEEC8DAE39C24B
SHA1:	4C021B1060F156AA0CF367BEEFACF97CE023266C
SHA-256:	FC81DD32E4E7FB2C1D1FFFCDCB8B3856DE18807EA6D585FF4C8366767CF43CE6
SHA-512:	F95BDC00338820478A54FE3BB9A4A929A7EB040120ACFAC891245C9C667F14BDFA45CA2C5306A3E688F3C79A391314528AAA7C88FAAE8F64E58ADB763AF62CA3
Malicious:	false
Reputation:	unknown
Preview:	ZGGKN.+.h.....'.D=...+/w>.XFt.....&|..'....o.....dY..z.~...i3y...5M...G..$.t.2.....kGG.I...hj...]EmJI....h....wP.Hi...9....=.=.@C:...\..2....p.....2]t..E...^.K...m..O..N..t..z ..u..WQ.y.o}+A..E.>.....~.Nf. _...T.c.....\|8..q.r1C.I...]..f....<..!.T.5..]....I.,.x@..O..gm.....fh@.hQ...U.L..X\...7A0.2..>e.5..`.'.M.....w.....O.....1.6H...."H{..l.1.px.x.5GFoU3... .y.'.....y<.*.T..S..xE.....t..@.Gl.z2.....W".G\|..}.....%..'7..:[.f.:W..m....p..\..1y....1....$..5H.!..Y9KP.R.1_...P%O==*.d.N.....c'..i{.J.-.k..iX...B.b%<\q.....N...|..L[[..(..5.^.y....yQ.'7..? =9..\....0....v.U.FKV,.-.MR.Q7..P.e.].....I.A.h..m...(.}(.K.....r4. .i...W.D.6.be.=.....g..t..d..)....i.....k+.fW.V.7.%.F...?.....q.+!=?.U..-U..... ..*.F..T.....LL..V.$.r...a9mC@.y...(.... f.wy(-..aF.g6u..n.tP...T5..`..j.....&.Z.].0.y..l.z.....[....8,.q.,....R.L.m...+'.Z..k..^.J(...b.1S.....?.4...J.....t...Q.....4j..j.x.....So.J.X..l.....<.....M..<n.

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.832484974145176
Encrypted:	false
SSDEEP:	24:ol08RQcT8W/5aF7WsSFczGqdv4CeYB58LZepjW15D+UxSkvQukrzAO4GbD:MQcd/kBCkGqK7g58LZeF65DHVQRzAxUD
MD5:	034F1165D88F988B8F15019C10CA9BDA
SHA1:	9A654FBADB33CC0C6B7FD9A9A295EC7464C1A446
SHA-256:	C2B8C4F7905BFE80C091D0229AB48610F91ED895617A2BAD7D59331CEA1961F6
SHA-512:	12CF316A0258643F1ED5CD75ED27635D990C3EC39B8B862EE97833D41773B7DDA33F2F7BCDAF0C4B0FAE677C1C5FCFB7152392146112 71BFDF979B31D9C621A
Malicious:	false
Reputation:	unknown
Preview:	EWZCV.:.I...C..5..x..=...;z..NF.KYth..Tsl..s].....|.>..}2k.!....*.q<.....X...C-.).YrEz..s..>5.F.lCu..)...6..oI...i.Xg(.X.....y..%.E.....z..P.r.v...).} ..8.....c..f.P..$..~b..$.Ns.....Z..L..y. ..>.....J.iB53.o...+h:..1.r8...1.k....W>^qr..=.*....pp...../4.....B...0e&$..~8.*.NArV.._.%*9;.....k.:3uQs...NZ..F.....3)m.\...A.Q.....s.G2."{.{Q.9N.4.F.,...h\~..:e.f.:.. UV.(..z...Z .....y.9..w.~..Rp....6B..x.....w.J.G.u.0. v.$...X.:..j....k...~[.W}.._(.B.iz..I.]...>....d.....,.....X..b...=.....5.V2..Zf..ML...YkV...L..QH...9....z1H..Xx...j._$}^:..1.F..V".....o...)K.L/...]y..... !...H.D../...y..T.\|..v.Z.].....rY..2..0..S..v.J..yk..L.%B3x.a....u...a..... Vc.R.-....5....<.ECV...aIB7K..'....{.7.F.%..0..]@..J.+..ia.#....X.[.B1.\|(..d\@(...4{.>.$.#.y.b.)?W.....%".. !.RBy.m.....X.i.a..C..^a.....^..g.o..V.L..s..k&.a...-.Q..-.L3.w.i....w[...N,.0.j.j7H..^\...l.c+.*._.2....Uc5..'.....q.6|@.....;8i..#4.....B...Z...'.'.Flap.

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.832484974145176
Encrypted:	false
SSDEEP:	24:ol08RQcT8W/5aF7WsSFczGqdv4CeYB58LZepjW15D+UxSkvQukrzAO4GbD:MQcd/kBCkGqK7g58LZeF65DHVQRzAxUD
MD5:	034F1165D88F988B8F15019C10CA9BDA
SHA1:	9A654FBADB33CC0C6B7FD9A9A295EC7464C1A446
SHA-256:	C2B8C4F7905BFE80C091D0229AB48610F91ED895617A2BAD7D59331CEA1961F6
SHA-512:	12CF316A0258643F1ED5CD75ED27635D990C3EC39B8B862EE97833D41773B7DDA33F2F7BCDAF0C4B0FAE677C1C5FCFB7152392146112 71BFDF979B31D9C621A
Malicious:	false
Reputation:	unknown

Preview:	EWZCV.:.I...C..5..x..=...;z..NF.KYth..Tsl..s].....|.>..}2k.!....*.q<.....X...C-.).YrEz..s..>5.F.lCu..)...6..oI...i.Xg(.X.....y..%.E.....z..P.r.v...).} ..8.....c..f.P..$..~b..$.Ns.....Z..L..y. ..>.....J.iB53.o...+h:..1.r8...1.k....W>^qr..=.*....pp...../4.....B...0e&$..~8.*.NArV.._.%*9;.....k.:3uQs...NZ..F.....3)m.\...A.Q.....s.G2."{.{Q.9N.4.F..,...h\~..:e.f.:.. UV.(..z...Z .....y.9..w.~..Rp....6B..x.....w.J.G.u.0. v.$...X.:..j....k...~[.W}.._(.B.iz..l.]...>....d.....,....X..b...=.....5.V2..Zf..ML...YkV...L..QH...9....z1H..Xx...j._$}^:..1.F..V".....o...)K.L/...]y..... !...H.D../...y..T.|..v.Z.].....rY..2..0..S..v.J..yk..L.%B3x.a....u...a..... Vc.R.-....5....<.ECV...aIB7K..'....{.7.F.%..0..]@..J.+..ia.#....X.[.B1.|(..d\@(...4{.>.$.#.y.b.)?W.....%".. !.RBy.m.....X.i.a..C..^a.....^..g.o..V.L..s..k&.a...-.Q..-.L3.w.i....w[...N,.0.j.j7H..^\...l.c+.*._.2....Uc5..'.....q.6|@.....;8i..#4.....B...Z...''.Flap.

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.841841333298593
Encrypted:	false
SSDEEP:	24:643fd9zOH1rkZoLx60wpGHeulyTh9laaU030wGOPNJAU5mhS5IpbD:64vdQ1kZWMtPu4Jp93j3bgmlJD
MD5:	E7C7E0C776D1F9E880D83D78726802E6
SHA1:	959B6F5C4624705318E5F7CCACCE7110DD6C3EFE
SHA-256:	89AAC2F03283163625EDBBA8BDEA5257EADDA7C3CEA8D3A7C753AD7388E31DE1
SHA-512:	62EB443D0603CA6C7C30B0CC6A41E12D308F5DCECA8F04748ACD71F40A32B12FEC479AFC1F9AA8523F7211C59D8B08B2F311A818FA43186A2A9F535ED665183
Malicious:	false
Reputation:	unknown
Preview:	EWZCV.lj..%....(ICe..w.5P5...r.......fL..+..8..7Q.H.VB...Z..X/.U....-.-%f....j../.4s.|..&...1I..F.......O...^}..O.}...I.<...6i.Z9Gr...(.a...I .....*.dq.t.....!%q..ZU.4<.I<1.<.t...r~.....$.\A.x...R..qO..}..U..|i.}.~.]..[%..~....91E.mj@u7b.....E....b.|.k@<X.Y>.....J.e...f.m....(7.'1.M..(...s...g.|..o.F..Wxqi4.....c<.~,D...I.v. ...]....k8..).,. $...E..9^Q.....l...}.+~.5CH..u...\.. <....z...-..Dd.+....d#...9z-.0..(?Q...0 4t..d(.e.....X..A%...r..O6*|.~E&.(...x(....C.Y./..m.b..=..{.....C#._...Y....-I.(@5.G.my.y...6K.^x..?}C"...U...J..'.p....B.....]W.I2s.../..R7.`..b..... 3J..=E..5.....4.I...A..?w.`R.&.....NG>.C.....g...wT.'.>.f.zk..o....C..,...l..&$.....X.,....S...9..F....Z..6..N_..r).:,e;.X{!.E}.D..oh{-.7E.h..\.4..v.]..x..u.z..3.&.."x=.}..#.rP/.K.4.- ..3_r.^r.g..;...LZ{...1t..G...c!R.*-..V.WL!...V...Hn..&.m..._q..q.[-....q.C}.9..pu...MH..,>.&I.Q._Hy. ..X.I.s5...b..3...m...k.)....E.Qa...W#.I.O..\+.p..V:..-.<.-..Z...

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.841841333298593
Encrypted:	false
SSDEEP:	24:643fd9zOH1rkZoLx60wpGHeulyTh9laaU030wGOPNJAU5mhS5IpbD:64vdQ1kZWMtPu4Jp93j3bgmlJD
MD5:	E7C7E0C776D1F9E880D83D78726802E6
SHA1:	959B6F5C4624705318E5F7CCACCE7110DD6C3EFE
SHA-256:	89AAC2F03283163625EDBBA8BDEA5257EADDA7C3CEA8D3A7C753AD7388E31DE1
SHA-512:	62EB443D0603CA6C7C30B0CC6A41E12D308F5DCECA8F04748ACD71F40A32B12FEC479AFC1F9AA8523F7211C59D8B08B2F311A818FA43186A2A9F535ED665183
Malicious:	false
Reputation:	unknown
Preview:	EWZCV.lj..%....(ICe..w.5P5...r.......fL..+..8..7Q.H.VB...Z..X/.U....-.-%f....j../.4s.|..&...1I..F.......O...^}..O.}...I.<...6i.Z9Gr...(.a...I .....*.dq.t.....!%q..ZU.4<.I<1.<.t...r~.....$.\A.x...R..qO..}..U..|i.}.~.]..[%..~....91E.mj@u7b.....E....b.|.k@<X.Y>.....J.e...f.m....(7.'1.M..(...s...g.|..o.F..Wxqi4.....c<.~,D...I.v. ...]....k8..).,. $...E..9^Q.....l...}.+~.5CH..u...\.. <....z...-..Dd.+....d#...9z-.0..(?Q...0 4t..d(.e.....X..A%...r..O6*|.~E&.(...x(....C.Y./..m.b..=..{.....C#._...Y....-I.(@5.G.my.y...6K.^x..?}C"...U...J..'.p....B.....]W.I2s.../..R7.`..b..... 3J..=E..5.....4.I...A..?w.`R.&.....NG>.C.....g...wT.'.>.f.zk..o....C..,...l..&$.....X.,....S...9..F....Z..6..N_..r).:,e;.X{!.E}.D..oh{-.7E.h..\.4..v.]..x..u.z..3.&.."x=.}..#.rP/.K.4.- ..3_r.^r.g..;...LZ{...1t..G...c!R.*-..V.WL!...V...Hn..&.m..._q..q.[-....q.C}.9..pu...MH..,>.&I.Q._Hy. ..X.I.s5...b..3...m...k.)....E.Qa...W#.I.O..\+.p..V:..-.<.-..Z...

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

Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.830861793145688
Encrypted:	false
SSDEEP:	24:jwKHWzFk1i5WAaQTfH2n+8F5DGapAJWgaewhVpJYg5cNBT4BNHY3OVsw0bD:0FzLWAaQJnuewhxqedvedD
MD5:	F18C2754099B8A648F7746D168AE558F
SHA1:	353675EBB0C169F2A73AC49523927A7E9F5CAE9E
SHA-256:	87A4C1B345DDB7BBF086B708D374169BC4E53323486942B06B3DF502797D9B20
SHA-512:	7B79EDC75D232FFBE1C3D2CB22F3C8F02E0080C18067C6AB452BA63D09F4A4C36A42AA5C2E42F2B37AA49E5E869F0C57B1E40216B3D1D4110E684FA50D5B0911
Malicious:	false
Reputation:	unknown

Preview:	GIGIY..a.t{.!...l.|i...y..../$.....Yl.k}.7.Q_z.@.....hT...J..l.W,.%.#.u@..."l.j-..F..*.....E..%.+..w..4..[&>.y...)S}t...i.....|.....,7.]..0.5Vqs..g.b.v._}y..j.uc&...Kx...'.o...<.....G.Gi.5.....z... ...l/[n...a.}.R....)=.q8m.\s%.2V...g.$.{}.(Y...F.L....:.z.}...N.w...M..z.Vq.....P.6U&j..f..?..W....;.U.m.i.X...n..oj.x....o..Qc..K..pQ.I5.S..L.....j..jl.r.-.C.[#..a.i.:..0...o..Y..3..~...!~S...hc.3. ..9.F].0..B..f.%h.....rn$.y..E..l]4.g>.Z.w..p....[g..A.t.z..F5..$t#-....<...9...!+.c..y>.t...80..D.Ed=.X.....f.....74.mI...$ .0#^....i...a..Z...|...;|Q.q.H1.j...Ox5..w49.....^.#S7 .....h.a.%..B..+|.0..>....".1.X#A[G....XuA...r..F..s..).8)E..4.....T...9..S|'...wW.....<.....&...=..P.....<7.%.Q..U.....4./..1..{.....\.y...tl.b!...\.a.iC.\\....Q..\...p...Qc!;\.d.....:.5q.. .....w.2W....T.i.aZce...T.h.8..>.!1...J..Z.Cnrd..#@...I..2.E.\p._Ht.f..$'.'.8..^@.....p:2.q6.g.d.0.dS....ucd.s.A..m.u...%.....p".....[.....T..!....P

C:\Users\user\Desktop\GIGIYTFFYT.png.vapo (copy)	
Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.830861793145688
Encrypted:	false
SSDEEP:	24:jwKHWzFk1i5WAaQTfH2n+8F5DGapAJWgaewhVpJYg5cNBT4BNHY3OVsw0bD:0FzLWAaQJnuewhxqedvedD
MD5:	F18C2754099B8A648F7746D168AE558F
SHA1:	353675EBB0C169F2A73AC49523927A7E9F5CAE9E
SHA-256:	87A4C1B345DDB7BBF086B708D374169BC4E53323486942B06B3DF502797D9B20
SHA-512:	7B79EDC75D232FFBE1C3D2CB22F3C8F02E0080C18067C6AB452BA63D09F4A4C36A42AA5C2E42F2B37AA49E5E869F0C57B1E40216B3D1D4110E684FA50D5B09 11
Malicious:	false
Reputation:	unknown
Preview:	GIGIY..a.t{.!...l.|i...y..../$.....Yl.k}.7.Q_z.@.....hT...J..l.W,.%.#.u@..."l.j-..F..*.....E..%.+..w..4..[&>.y...)S}t...i.....|.....,7.]..0.5Vqs..g.b.v._}y..j.uc&...Kx...'.o...<.....G.Gi.5.....z... ...l/[n...a.}.R....)=.q8m.\s%.2V...g.$.{}.(Y...F.L....:.z.}...N.w...M..z.Vq.....P.6U&j..f..?..W....;.U.m.i.X...n..oj.x....o..Qc..K..pQ.I5.S..L.....j..jl.r.-.C.[#..a.i.:..0...o..Y..3..~...!~S...hc.3. ..9.F].0..B..f.%h.....rn$.y..E..l]4.g>.Z.w..p....[g..A.t.z..F5..$t#-....<...9...!+.c..y>.t...80..D.Ed=.X.....f.....74.mI...$ .0#^....i...a..Z...|...;|Q.q.H1.j...Ox5..w49.....^.#S7 .....h.a.%..B..+|.0..>....".1.X#A[G....XuA...r..F..s..).8)E..4.....T...9..S|'...wW.....<.....&...=..P.....<7.%.Q..U.....4./..1..{.....\.y...tl.b!...\.a.iC.\\....Q..\...p...Qc!;\.d.....:.5q.. .....w.2W....T.i.aZce...T.h.8..>.!1...J..Z.Cnrd..#@...I..2.E.\p._Ht.f..$'.'.8..^@.....p:2.q6.g.d.0.dS....ucd.s.A..m.u...%.....p".....[.....T..!....P

C:\Users\user\Desktop\HMPPSXQPQV.mp3	
Process:	C:\Users\user\AppData\Local\Temp\BDC0.exe
File Type:	data
Category:	dropped
Size (bytes):	1360
Entropy (8bit):	7.851677439083383
Encrypted:	false
SSDEEP:	24:7zzo8pI9IBWNhVIt1IEjHy8C3br+MEaLQaDdzaElmUjC8qkGmuEDA9SNfCDwjDlc:f/m9Iy0t4jHybGMEaL1xuc5TqkGmNDAH
MD5:	492AED3E0BC9EF043681E2B5A4C025BA
SHA1:	6959C039E130ACA484BECF5C2E4B9508B5B5938C
SHA-256:	BDC829978EB8E13F02D5B75CA63BD91C2D653665D2A13C6C291B0746CB8B6B39
SHA-512:	DC8AE48E894F6F75422789D88432CE43504CA476F40F10CB2FF54DC844E7346217E46032F2CED72CE765C5AA03328F340FC5E4A31FBAA5A3A41C35875258877A
Malicious:	false
Reputation:	unknown
Preview:	HMPPSJ-W.a.x.E..+.P.....:.`...?5m.r-.[G.byT..._.o....].W.bYo..|..'..W.(.....hnWMZ...B.*=.Y..,..T...T..E.....-..[..r$c...V...Z....[.&..c.a.8c.?].B..J#....h..S...*...\..}...I8....S...<.Dr.... ..DW.g..j.....x..}s!?.Z..V..0.=....p..-....5.....w.H...^]`<n..{?.....y...2K.w..sbl.B.Z...lz.....s..K..f.v.+-...dpX.1..j.vN.....:...z..r.Dn.v..^o..J.....!X...6..?~.G..3..m]+.m?.."a:.? .q.b)...P{.a?.)..... i.a.M=V...?x..+d.,n. ...T6-.>9.a..L.j_...m.....)t..wT.....2...i.l.m.....b..9N.k...'S_V..3....P...Xl%.W..)`....jOs..|4...((..2.2.....}.~...../..}.....6.Ps~.!....R.x..^ ..R..|C.....:k.5.]...W@..`...!...,.chH....hz....c..(>...R.t..<....Y.i.....=.....'"..Vw.%..!..'....hLn..~...J...+E9... .....Uv!jI..E$l..^..7I.Vl2..c.h.*}.....Q..+...&..0ta..t.J.@.....O. b.W/.....jG'.`. .CSk$!g...?.H../..6k.U.igu. ...[..:la....h,...F.5%.q.....Vu.z]'/...re?.....o....V.....L.....8X.....1.H5...}..\...+K.C.>ue.0x.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.603075701960206
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:	02107799.exe
File size:	282112
MD5:	6017e7c6f19de9e3b0aae0965fe25603
SHA1:	605250b6dabafb86252272b757a1713078c6ae79
SHA256:	c421418b410ea4bf78ef47c8edb75c8fc96220043573ba6d8268bca900a4c041
SHA512:	da62cab044a336881f388e93495ed9bc6aa6d1559556de0efe8585b932a3e12c7a20322e913fb0fa8b3c402b119d5924efc6fe51550ac95c2967713a0b0b0ed1

SSDEEP:	3072:kKAuVGwBlcQlbzjmj7FHmfuzv+ippcQPd5gG+LGvAcYWt:9AuVGhQlbzUw+5XcPGmvW
TLSH:	BD543B1396E2BC54FD668B729E2FC6EC761DB1A28F19776932184A2F04702B2D173713
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.....b.....

File Icon

Icon Hash:	554555454545691d

Static PE Info

General

Entrypoint:	0x404dd9
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x6297F6D6 [Wed Jun 1 23:31:34 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:	d302e4ac3406067f8ed838633897aebb

Entrypoint Preview

Instruction
call 00007F1354CE7033h
jmp 00007F1354CE26CDh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F1354CE2876h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F1354CE28A0h
test ecx, 00000003h
jne 00007F1354CE2841h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]

Instruction
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 00007F1354CE283Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F1354CE2884h
test ah, ah
je 00007F1354CE2876h
test eax, 00FF0000h
je 00007F1354CE2865h
test eax, FF000000h
je 00007F1354CE2854h
jmp 00007F1354CE281Fh
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	0x283a8	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x26f000	0x17700	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x287000	0xdf4	.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	0x30c8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
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	0x27e62	0x28000	False	0.785137939453125	data	7.578116721772191	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	0x17700	0x17800	False	0.3848175698138298	DIY-Thermocam raw data (Lepton 3.x), scale -32383-32383, spot sensor temperature -0.000000, unit celsius, color scheme 0, calibration: offset 1701411834604692317316873037158841057 28.000000, slope 3382859084964222185885342076459317985 28.000000	4.2257902008995	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x287000	0x331e	0x3400	False	0.22611177884615385	data	2.5288792513598777	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x26f6d0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x26fd98	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x272340	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x2727d8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x273680	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x273f28	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x274490	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x276a38	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x277ae0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x278468	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x278938	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x2797e0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x27a088	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x27a750	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x27acb8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x27d260	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x27e308	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x27e7d8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x27f680	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x27ff28	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x280490	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x282a38	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x283ae0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x284468	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_STRING	0x284b70	0x6fa	data		
RT_STRING	0x285270	0x6a8	data		
RT_STRING	0x285918	0x4b8	data		
RT_STRING	0x285dd0	0x1da	data		
RT_STRING	0x285fb0	0x74c	data		
RT_GROUP_ICON	0x2848d0	0x68	data		
RT_GROUP_ICON	0x27e770	0x68	data		
RT_GROUP_ICON	0x2727a8	0x30	data		
RT_GROUP_ICON	0x2788d0	0x68	data		
RT_VERSION	0x284938	0x234	data		

Imports

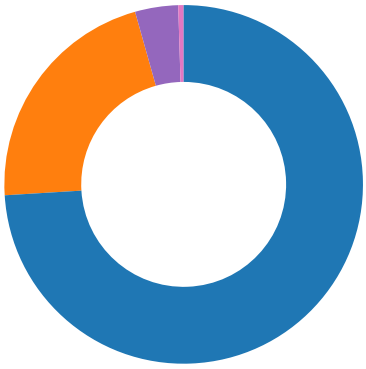
DLL	Import
KERNEL32.dll	GetModuleHandleW, GetTickCount, IsBadReadPtr, GetConsoleAliasesLengthA, GetPrivateProfileIntA, FreeConsole, GetVersionExW, WritePrivateProfileStructW, MulDiv, GetModuleFileNameW, CreateActCtxA, WritePrivateProfileStringW, ReplaceFileA, GetStringTypeExA, CreateJobObjectA, GetStdHandle, GetLogicalDriveStringsA, OpenMutexW, GetLastError, ReadConsoleOutputCharacterA, GetProcAddress, SleepEx, GetLongPathNameA, VirtualAlloc, EnterCriticalSection, _hwrite, LoadLibraryA, InterlockedExchangeAdd, LocalAlloc, GetFileType, CreateFileMappingW, FindFirstVolumeMountPointW, GetNumberFormatW, CreateEventW, GetModuleFileNameA, lstrcmpiW, GetModuleHandleA, CreateMutexA, GetFileAttributesExW, GetConsoleCursorInfo, ScrollConsoleScreenBufferA, FindAtomW, EnumResourceLanguagesW, DebugBreak, FindNextVolumeA, AddConsoleAliasW, CancelWaitableTimer, GetCommState, WaitForSingleObject, AttachConsole, GetCommandLineA, GetStartupInfoA, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, HeapFree, WideCharToMultiByte, SetHandleCount, DeleteCriticalSection, LeaveCriticalSection, Sleep, ExitProcess, WriteFile, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, InterlockedDecrement, HeapCreate, VirtualFree, QueryPerformanceCounter, 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

Skipped network analysis since the amount of network traffic is too extensive. Please download the PCAP and check manually.

Statistics

Behavior



- 02107799.exe
- explorer.exe
- cuwsgii
- BDC0.exe
- BDC0.exe
- AD22.exe
- icacls.exe
- svchost.exe
- WerFault.exe
- BDC0.exe
- WerFault.exe
- dllhost.exe
- BDC0.exe
- BDC0.exe
- BDC0.exe
- 223E.exe
- aafg31.exe
- NewPlayer.exe
- mnolyk.exe
- XandETC.exe
- schtasks.exe
- BDC0.exe
- conhost.exe
- cmd.exe
- conhost.exe
- 946D.exe
- BDC0.exe
- 946D.exe
- 8DD2.exe
- cmd.exe
- cacls.exe
- 794C.exe
- 8DD2.exe
- cacls.exe
- 794C.exe
- rundll32.exe
- DC0A.exe
- build2.exe
- rundll32.exe
- mnolyk.exe
- cmd.exe

Click to jump to process

System Behavior

Analysis Process: 02107799.exe PID: **7160**, Parent PID: **3324**

General

Target ID:	0
Start time:	10:43:57
Start date:	28/05/2023
Path:	C:\Users\user\Desktop\02107799.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\02107799.exe
Imagebase:	0x400000
File size:	282112 bytes
MD5 hash:	6017E7C6F19DE9E3B0AAE0965FE25603
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.397201524.0000000000840000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.397221431.0000000000871000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.397221431.0000000000871000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.397292566.0000000000939000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.397209073.0000000000850000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.397209073.0000000000850000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3324**, Parent PID: **7160**

General

Target ID:	1
Start time:	10:44:02
Start date:	28/05/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69bc80000
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

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: cuwsgii PID: **5704**, Parent PID: **1084**

General

Target ID:	4
Start time:	10:44:30
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Roaming\cuwsgii
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\cuwsgii
Imagebase:	0x400000
File size:	282112 bytes
MD5 hash:	6017E7C6F19DE9E3B0AAE0965FE25603
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: 00000004.00000002.460136042.00000000007E0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000002.460449041.00000000022E1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000004.00000002.460449041.00000000022E1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000002.460185114.00000000007F0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000004.00000002.460185114.00000000007F0000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000004.00000002.460041377.00000000006E8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 38%, ReversingLabs
Reputation:	low

Analysis Process: BDC0.exe PID: **6912**, Parent PID: **3324**

General

Target ID:	5
Start time:	10:44:34
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\BDC0.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\BDC0.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: 00000005.00000002.453783695.0000000002510000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000005.00000002.453783695.0000000002510000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000005.00000002.453528210.00000000023BD000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: BDC0.exe PID: **7044**, Parent PID: **6912**

General

Target ID:	6
Start time:	10:44:35
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\BDC0.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\BDC0.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: 00000006.00000002.461344715.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000006.00000002.461344715.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000006.00000002.461344715.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000006.00000002.461344715.0000000000400000.00000040.00000400.00020000.00000000.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
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\9af1d69e-1bc5-4008-ad08-a746f07a48e8	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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.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\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.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 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\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.exe" --AutoStart	success or wait	1	4120F9	RegSetValueExW

Analysis Process: AD22.exe PID: **4724**, Parent PID: **3324**

General

Target ID:	7
Start time:	10:44:36
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\AD22.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\AD22.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: 00000007.00000002.466741568.00000000006E0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000007.00000002.466859544.0000000000818000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: icacls.exe PID: **4744**, Parent PID: **7044**

General

Target ID:	8
Start time:	10:44:36
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	icacls "C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8" /deny *S-1-1-0:(OI)(CI)(DE,DC)
Imagebase:	0x8f0000
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	84			invalid handle	1	8F1B0A	WriteFile
unknown	unknown	59			invalid handle	1	8F1B0A	WriteFile

Analysis Process: svchost.exe PID: **3276**, Parent PID: **564**

General

Target ID:	9
Start time:	10:44:36
Start date:	28/05/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6ffff0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	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: WerFault.exe PID: **256**, Parent PID: **3276**

General

Target ID:	10
Start time:	10:44:37
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 4724 -ip 4724
Imagebase:	0x330000
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: BDC0.exe PID: **4248**, Parent PID: **1084**

General

Target ID:	11
Start time:	10:44:37
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.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: 0000000B.00000002.463353305.000000000232B000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000B.00000002.463587041.0000000002480000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000B.00000002.463587041.0000000002480000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: WerFault.exe PID: **3356**, Parent PID: **4724**

General

Target ID:	12
Start time:	10:44:37
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4724 -s 520
Imagebase:	0x330000
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	6C241717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6CA9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6CA9.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C23497A	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_AD22.exe_bc3690d31fe876d95d6ec65d5dc56974b7b47db_5f8597d0_0d70ed7f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_AD22.exe_bc3690d31fe876d95d6ec65d5dc56974b7b47db_5f8597d0_0d70ed7f\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C23497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6CA9.tmp	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp.dmp	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6CA9.tmp.xml	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6CB6.tmp.csv	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E3E.tmp.txt	success or wait	1	6C23497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 06 fd 73 64 fd 05 12 00 00 00 00 00	MDMP sd	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp.dmp	5944	6	00 00 00 00 00 00		success or wait	1	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.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 74 12 00 00 04 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	UB8GenuineIntelWTtsd Pacific Standard TimePacific Daylight Time	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.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 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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp.dmp	1620	168	6c 12 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 fd 02 00 00 fd 1a 00 00	lgg	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp.dmp	9730	20	0e 00 00 00 fd fd fd 00 00 00 00 00 3c 02 00 00 fd 26 00 00	<&	success or wait	14	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp.dmp	9958	572	fd fd 0f 77 fd fd 0d 77 fd 00 00 00 fd fd fd fd 10 00 00 00 58 fd fd 00 24 fd fd 00 fd fd fd fd 40 fd 0d 77 40 fd 0d 77 fd fd fd fd 00 30 26 00 00 30 26 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 30 26 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 6e 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 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 40 12 fd 00 00 00 00 00 00 00 00 00 58 6a fd 00 00 fd 25 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd 54 fd 25 00 fd fd fd 00 fd 6e fd 00 fd fd fd 00 00 00 00 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	wwX$@w@w0&0&0&n@Xj%T%n	success or wait	13	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.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 33 76 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 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 00 00 0e fd fd 73 fd fd fd fd 00 00 00 00 fd fd 19 00 fd 40 fd 72 fd fd fd fd fd fd fd fd fd 19 00 fd fd 0c 77 fd fd 19 00 fd fd fd fd 60 fd 6d 76 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 54 fd 0c 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 fd	(8!3v@@s@rw`mvTw	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.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 fd fd	?+S++,@@g#F+	success or wait	3	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp.dmp	1888	48	fd 11 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 30 26 00 00 00 00 00 fd fd fd 00 00 00 00 00 3c 02 00 00 fd 26 00 00 fd 02 00 00 36 23 00 00	0&<&6#	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp.dmp	1948	4	1f 00 00 00		success or wait	31	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp.dmp	5950	22	10 00 00 00 41 00 44 00 32 00 32 00 2e 00 65 00 78 00 65 00 00 00	AD22.exe	success or wait	31	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.tmp.dmp	5192	752	00 00 fd 75 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 fd fd 02 00 00 00 00 00 fd 46 03 00 00 00 00 32 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 3a fd 03 00 00 00 00 00 33 1e 04 00 00 00 00 00 00 00 00 00 00 00 00 00 43 fd 1a 00 00 00 00 00 fd 4d 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 5b 05 00 00 00 00	u8 BB? #@AZbF2:3CM@[	success or wait	1	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6AE2.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.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	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 34 00 37 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4724</Pid>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 41 00 44 00 32 00 32 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>AD22.exe</ImageName>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1072	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1170	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 36 00 35 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1650</Uptime>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1212	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1216	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1220	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1302	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1306	2	09 00		success or wait	2	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1310	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1362	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1366	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1370	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1414	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1418	2	09 00		success or wait	3	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1424	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1510	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1514	2	09 00		success or wait	3	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1520	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1590	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1594	2	09 00		success or wait	3	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1600	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 38 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>2338</PageFaultCount>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1674	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1678	2	09 00		success or wait	3	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1684	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1780	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1784	2	09 00		success or wait	3	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1790	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1870	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1874	2	09 00		success or wait	3	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1880	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1994	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	1998	2	09 00		success or wait	3	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2004	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2102	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2106	2	09 00		success or wait	3	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2112	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 38 00 31 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 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>37816</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2236	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2240	2	09 00		success or wait	3	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2246	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 38 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>37680</QuotaNonPagedPoolUsage>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2354	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2358	2	09 00		success or wait	3	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2364	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 32 00 33 00 39 00 36 00 38 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>3923968</PagefileUsage>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2440	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2444	2	09 00		success or wait	3	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2450	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 38 00 30 00 36 00 34 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>3928064</PeakPagefileUsage>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2542	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2546	2	09 00		success or wait	3	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2552	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 32 00 33 00 39 00 36 00 38 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>3923968</PrivateUsage>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2624	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2628	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2632	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2678	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2682	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2686	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2716	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2720	2	09 00		success or wait	3	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2726	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2766	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2770	2	09 00		success or wait	4	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2778	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2808	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2812	2	09 00		success or wait	4	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2820	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2890	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2894	2	09 00		success or wait	4	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2902	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2992	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	2996	2	09 00		success or wait	4	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3004	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 35 00 34 00 30 00 36 00 34 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6540648</Uptime>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3052	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3056	2	09 00		success or wait	4	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3064	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3154	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3218	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3276	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3366	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3370	2	09 00		success or wait	5	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3380	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3454	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3458	2	09 00		success or wait	5	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3468	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 33 00 38 00 35 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>153855</PageFaultCount>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3546	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3550	2	09 00		success or wait	5	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3560	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 37 00 39 00 30 00 37 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>156790784</PeakWorkingSetSize>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3660	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3664	2	09 00		success or wait	5	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3674	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 35 00 36 00 36 00 34 00 33 00 33 00 32 00 38 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>156643328</WorkingSetSize>	success or wait	1	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3758	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3762	2	09 00		success or wait	5	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3772	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 37 00 39 00 34 00 38 00 30 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>1179480</QuotaPeakPagedPoolUsage>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3888	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3892	2	09 00		success or wait	5	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	3902	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 35 00 34 00 31 00 37 00 36 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>1154176</QuotaPagedPoolUsage>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4002	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4006	2	09 00		success or wait	5	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4016	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 32 00 32 00 32 00 38 00 38 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 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>222888</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4156	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 38 00 39 00 39 00 36 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>89960</QuotaNonPagedPoolUsage>	success or wait	1	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4278	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 35 00 32 00 31 00 32 00 35 00 36 00 39 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>5212569 6</PagefileUsage>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4370	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 32 00 31 00 32 00 35 00 36 00 39 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>52 125696</P eakPagefileUsage>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4478	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 35 00 32 00 31 00 32 00 35 00 36 00 39 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>5212569 6</PrivateUsage>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4564	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4620	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4670	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4708	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4756	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4802	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	9	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	18	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	4862	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 41 00 44 00 32 00 32 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>AD22.exe</Parameter0>	success or wait	9	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	5570	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	5574	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	5576	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	5616	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	5620	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	5622	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	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	5660	4	0d 00 0a 00		success or wait	6	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	5664	2	09 00		success or wait	12	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	5668	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6222	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6226	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6228	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6268	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6272	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6274	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6312	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6316	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6320	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6414	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6418	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6422	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 73 00 75 00 77 00 63 00 64 00 63 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>suwcdc, Inc.</SystemManufacturer>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6528	4	0d 00 0a 00		success or wait	1	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6532	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6536	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 73 00 75 00 77 00 63 00 64 00 63 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>suwcdc7,1</SystemProductName>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6640	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6760	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6764	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6768	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 34 00 36 00 31 00 30 00 30 00 31 00 30 00 39 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>1634610109</OSInstallDate>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6850	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6854	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6858	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6960	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6964	2	09 00		success or wait	2	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	6968	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7036	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7040	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7042	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7082	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7086	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7088	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7122	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7126	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7130	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</UEFISecureBootEnabled>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7226	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7230	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7232	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7268	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7272	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7274	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7298	4	0d 00 0a 00		success or wait	3	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7302	2	09 00		success or wait	6	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7306	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7550	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7554	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7556	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7582	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7586	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7588	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 34 00 3a 00 33 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-28T17:44:38Z">	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7688	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7692	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7696	258	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 38 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 37 00 32 00 34 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 33 00 37 00 34 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 33 00 37 00 34 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	<Process AsId="385" PID="4724" UptimeMS="374" TimeSinceCreationMS="374" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7954	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7958	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7962	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	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7982	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7986	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	7988	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	8026	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	8030	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	8032	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	8070	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	8074	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	8078	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 35 00 64 00 36 00 62 00 31 00 63 00 32 00 2d 00 32 00 62 00 32 00 61 00 2d 00 34 00 37 00 30 00 35 00 2d 00 62 00 63 00 33 00 62 00 2d 00 36 00 63 00 32 00 32 00 66 00 39 00 37 00 34 00 31 00 66 00 66 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>55d6b1c2-2b2a-4705-bc3b-6c22f9741ffc</Guid>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	8176	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	8180	2	09 00		success or wait	2	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	8184	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 34 00 3a 00 33 00 38 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>2023-05-28T17:44:38Z</CreationTime>	success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	8282	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	8286	2	09 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	8288	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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	8328	4	0d 00 0a 00		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C3A.tmp.WERInternalMetadata.xml	8332	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	6C23497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6CA9.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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_AD22.exe_bc3690d31fe876d95d6ec65d5dc56974b7b47db_5f8597d0_0d70ed7f\Report.wer	0	2	fd fd		success or wait	1	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_AD22.exe_bc3690d31fe876d95d6ec65d5dc56974b7b47db_5f8597d0_0d70ed7f\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	6C23497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_AD22.exe_bc3690d31fe876d95d6ec65d5dc56974b7b47db_5f8597d0_0d70ed7f\Report.wer	10082	44	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 36 00 32 00 39 00 38 00 38 00 30 00 35 00 30 00 33 00	MetadataHash=629880503	success or wait	1	6C23497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: dllhost.exe PID: **5456**, Parent PID: **788**

General

Target ID:	14
Start time:	10:44:38
Start date:	28/05/2023
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}
Imagebase:	0x7ff7528c0000
File size:	20888 bytes
MD5 hash:	2528137C6745C4EADD87817A1909677E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: BDC0.exe PID: **5484**, Parent PID: **4248**

General

Target ID:	17

Start time:	10:44:39
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.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: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000011.00000002.895547083.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000011.00000002.895547083.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000011.00000002.895547083.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000011.00000002.895547083.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

Analysis Process: BDC0.exe PID: **1516**, Parent PID: **7044**

General	
Target ID:	18
Start time:	10:44:38
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\BDC0.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\BDC0.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: 00000012.00000002.463532414.0000000002410000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000012.00000002.463532414.0000000002410000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000012.00000002.463290987.0000000002349000.00000040.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: BDC0.exe PID: **2900**, Parent PID: **1516**

General	
Target ID:	19
Start time:	10:44:39
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\BDC0.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\BDC0.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: 00000013.00000002.895386251.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000013.00000002.895386251.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000013.00000002.895386251.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000013.00000002.895386251.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

Analysis Process: 223E.exe PID: **2952**, Parent PID: **3324**

General

Target ID:	20
Start time:	10:44:42
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\223E.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\223E.exe
Imagebase:	0x700000
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: 00000014.00000002.513841779.00000000040C5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_DLInjector04, Description: Detects downloader / injector, Source: C:\Users\user\AppData\Local\Temp\223E.exe, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 70%, ReversingLabs

Analysis Process: aafg31.exe PID: **2280**, Parent PID: **2952**

General

Target ID:	21
Start time:	10:44:44
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:	0x7ff6607d0000
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: **2284**, Parent PID: **2952**

General

Target ID:	22
Start time:	10:44:44
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:	0xff0000
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: 00000016.00000000.473283405.0000000000FF1000.00000020.00000001.01000000.00000011.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000016.00000002.476001535.0000000000FF1000.00000020.00000001.01000000.00000011.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: mnolyk.exe PID: **6916**, Parent PID: **2284**

General

Target ID:	23
Start time:	10:44:45
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:	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, Description: Yara detected Amadey bot, Source: 00000017.00000003.507221089.0000000000877000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000017.00000000.475587099.0000000000061000.00000020.00000001.01000000.00000012.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: XandETC.exe PID: **4980**, Parent PID: **2952**

General

Target ID:	24
Start time:	10:44:46
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:	0x7ff6e4340000
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: schtasks.exe PID: **4696**, Parent PID: **6916**

General

Target ID:	25
Start time:	10:44:46
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\schtasks.exe

Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN mnolyk.exe /TR "C:\Users\user\AppData\Local\Temp\6d73a97b0c\mnolyk.exe" /F
Imagebase:	0x12c0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: BDC0.exe PID: **256**, Parent PID: **3324**

General

Target ID:	26
Start time:	10:44:46
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.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: 0000001A.00000002.500648966.00000000022CF000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000001A.00000002.502966627.0000000002470000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001A.00000002.502966627.0000000002470000.00000040.00001000.00020000.00000000.sdmp, Author: unknown

Analysis Process: conhost.exe PID: **1280**, Parent PID: **4696**

General

Target ID:	27
Start time:	10:44:47
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5052**, Parent PID: **6916**

General

Target ID:	28
Start time:	10:44:47
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /k echo Y|CACLS "mnolyk.exe" /P "user:N"&&CACLS "mnolyk.exe" /P "user:R" /E&&echo Y|CACLS "..\6d73a97b0c" /P "user:N"&&CACLS "..\6d73a97b0c" /P "user:R" /E&&Exit
Imagebase:	0x11d0000

File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4360**, Parent PID: **5052**

General

Target ID:	29
Start time:	10:44:48
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: 946D.exe PID: **2064**, Parent PID: **3324**

General

Target ID:	30
Start time:	10:44:48
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\946D.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\946D.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: 0000001E.00000002.490394408.00000000024B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001E.00000002.490394408.00000000024B0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000001E.00000002.489953243.000000000240F000.00000040.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: BDC0.exe PID: **5184**, Parent PID: **256**

General

Target ID:	31
Start time:	10:44:49
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\9af1d69e-1bc5-4008-ad08-a746f07a48e8\BDC0.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.00000002.497982449.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000001F.00000002.497982449.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000001F.00000002.497982449.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001F.00000002.497982449.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

Analysis Process: 946D.exe PID: **4576**, Parent PID: **2064**

General

Target ID:	32
Start time:	10:44:51
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\946D.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\946D.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: 00000020.00000002.509612718.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000020.00000002.509612718.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000020.00000002.509612718.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000020.00000002.509612718.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

Analysis Process: 8DD2.exe PID: **6048**, Parent PID: **3324**

General

Target ID:	33
Start time:	10:44:51
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\8DD2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8DD2.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: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000021.00000002.506259651.000000000234D000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000021.00000002.508427363.0000000002520000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000021.00000002.508427363.0000000002520000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 71%, ReversingLabs

Analysis Process: cmd.exe PID: **1092**, Parent PID: **5052**

General

Target ID:	34

Start time:	10:44:51
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" echo Y"
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cacls.exe PID: **3356**, Parent PID: **5052**

General

Target ID:	35
Start time:	10:44:51
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "mnolyk.exe" /P "user:N"
Imagebase:	0x60000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: 794C.exe PID: **5236**, Parent PID: **3324**

General

Target ID:	36
Start time:	10:44:51
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\794C.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\794C.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: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000024.00000002.497942098.00000000023CD000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000024.00000002.498086364.0000000002460000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000024.00000002.498086364.0000000002460000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 71%, ReversingLabs

Analysis Process: 8DD2.exe PID: **5312**, Parent PID: **6048**

General

Target ID:	37
Start time:	10:44:51
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\8DD2.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8DD2.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: 00000025.00000002.507378893.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000025.00000002.507378893.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000025.00000002.507378893.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000025.00000002.507378893.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

Analysis Process: cacls.exe PID: **4580**, Parent PID: **5052**

General

Target ID:	38
Start time:	10:44:52
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "mnolyk.exe" /P "user:R" /E
Imagebase:	0x60000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: 794C.exe PID: **5660**, Parent PID: **5236**

General

Target ID:	39
Start time:	10:44:52
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\794C.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\794C.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: 00000027.00000002.512282252.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000027.00000002.512282252.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000027.00000002.512282252.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000027.00000002.512282252.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

Analysis Process: rundll32.exe PID: **5672**, Parent PID: **6916**

General

Target ID:	40
Start time:	10:44:53
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\07c6bc37dc5087\cred64.dll, Main
Imagebase:	0x170000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: DC0A.exe PID: **4596**, Parent PID: **3324**

General

Target ID:	41
Start time:	10:44:53
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\Temp\DC0A.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\DC0A.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: 00000029.00000002.507218040.0000000000830000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000029.00000002.507218040.0000000000830000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000029.00000002.507318867.0000000002321000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000029.00000002.507318867.0000000002321000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000029.00000002.507033636.00000000006B8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000029.00000002.507203480.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: unknown

Analysis Process: build2.exe PID: **4724**, Parent PID: **2900**

General

Target ID:	42
Start time:	10:44:53
Start date:	28/05/2023
Path:	C:\Users\user\AppData\Local\205aa591-8aa8-4e2c-a5b1-c9b7aaf860cf\build2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\205aa591-8aa8-4e2c-a5b1-c9b7aaf860cf\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: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000002A.00000002.503393275.0000000000728000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000002A.00000002.506376694.00000000022F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 87%, ReversingLabs

Analysis Process: rundll32.exe PID: **5812**, Parent PID: **5672**

General	
Target ID:	43
Start time:	10:44:53
Start date:	28/05/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\07c6bc37dc5087\cred64.dll, Main
Imagebase:	0x7ff7c7d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: mnolyk.exe PID: **5892**, Parent PID: **1084**

General	
Target ID:	44
Start time:	10:44:53
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:	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: 0000002C.00000002.513002003.0000000000061000.00000020.00000001.01000000.00000012.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000002C.00000000.492656572.0000000000061000.00000020.00000001.01000000.00000012.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: **5536**, Parent PID: **5052**

General	
Target ID:	45
Start time:	10:44:53
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" echo Y"
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly