ID: 766457
Sample Name: kmxId0uLRn.exe
Cookbook: default.jbs
Time: 20:06:50
Date: 13/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

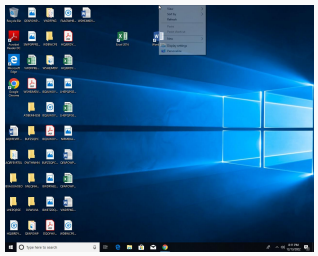
Windows Analysis Report

kmxId0uLRn.exe

Overview

General Information

Sample Name:	kmxId0uLRn.exe
Analysis ID:	766457
MD5:	c8782da2928f63..
SHA1:	0d87ba5d174405.
SHA256:	a68b2d14b767df..
Tags:	Dofoil, exe, SmokeLoader
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

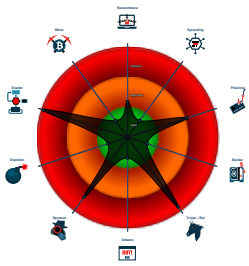
Amadey, SmokeLoader, Vidar

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

Signatures

- Yara detected Amadeys stealer DLL
- Yara detected SmokeLoader
- Yara detected Amadey bot
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Malicious sample detected (through…
- Yara detected Vidar stealer

Classification



Process Tree

- **System is w10x64**
- kmxId0uLRn.exe (PID: 5936 cmdline: C:\Users\user\Desktop\kmxId0uLRn.exe MD5: C8782DA2928F63712D03D0EA36C57C3F)
  - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - 8F68.exe (PID: 1568 cmdline: C:\Users\user\AppData\Local\Temp\8F68.exe MD5: 46F30465FA693033E7D3D78468406C0C)
      - conhost.exe (PID: 1324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - WerFault.exe (PID: 2292 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1568 -s 268 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - 9545.exe (PID: 6140 cmdline: C:\Users\user\AppData\Local\Temp\9545.exe MD5: C6524CC2CB091E23BE6D9526D6BCBC99)
      - gntuud.exe (PID: 5972 cmdline: "C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe" MD5: C6524CC2CB091E23BE6D9526D6BCBC99)
        - schtasks.exe (PID: 1012 cmdline: "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN gntuud.exe /TR "C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe" /F MD5: 15FF7D8324231381BAD48A052F85DF04)
          - conhost.exe (PID: 4944 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 504 cmdline: "C:\Windows\System32\cmd.exe" /k echo Y|CACLS "gntuud.exe" /P "user:N"&&CACLS "gntuud.exe" /P "user:R" /E&&echo Y|CACLS "..\2c33368f7d" /P "user:N"&&CACLS "..\2c33368f7d" /P "user:R" /E&&Exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - cmd.exe (PID: 4644 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Y" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - cacls.exe (PID: 3516 cmdline: CACLS "gntuud.exe" /P "user:N" MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
          - cacls.exe (PID: 5652 cmdline: CACLS "gntuud.exe" /P "user:R" /E MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
          - cmd.exe (PID: 5680 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Y" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - cacls.exe (PID: 5720 cmdline: CACLS "..\2c33368f7d" /P "user:N" MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
          - cacls.exe (PID: 5868 cmdline: CACLS "..\2c33368f7d" /P "user:R" /E MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
        - rundll32.exe (PID: 4876 cmdline: "C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll, Main MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - explorer.exe (PID: 2096 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 3940 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 1020 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 4044 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 4696 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 5536 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 5692 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 5896 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 1004 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- thgcici (PID: 2108 cmdline: C:\Users\user\AppData\Roaming\thgcici MD5: C8782DA2928F63712D03D0EA36C57C3F)
- gntuud.exe (PID: 3124 cmdline: C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe MD5: C6524CC2CB091E23BE6D9526D6BCBC99)
- thgcici (PID: 4892 cmdline: C:\Users\user\AppData\Roaming\thgcici MD5: C8782DA2928F63712D03D0EA36C57C3F)
- gntuud.exe (PID: 3920 cmdline: C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe MD5: C6524CC2CB091E23BE6D9526D6BCBC99)
- **cleanup**

Malware Configuration

Threatname: Amadey


```
{
  "C2 url": "62.204.41.79/fb73jc3/index.php",
  "Version": "3.60"
}
```


Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://s2scomm20.com/",
    "http://c2csosi228d.com/",
    "http://xdd42sdfsdf.com/"
  ]
}
```


Threatname: Vidar


```
{
  "C2 url": [
    "https://t.me/ttruelive",
    "https://steamcommunity.com/profiles/76561199443972360"
  ],
  "Botnet": "1808",
  "Version": "56.2"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Amadey	Yara detected Amadey bot	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	INDICATOR_TOOL_PWS_Amady	Detects password stealer DLL. Dropped by Amadey	ditekSHen	• 0xd868:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x15604:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x16074:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x15158:$s2: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook • 0x151bc:$s2: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook • 0xdd0c:$s3: \Mikrotik\Winbox\Addresses.cdb • 0x190d8:$s4: \HostName • 0x19100:$s5: \Password • 0x17c04:$s6: SOFTWARE\RealVNC\ • 0x17c30:$s6: SOFTWARE\RealVNC\ • 0x17c5c:$s6: SOFTWARE\RealVNC\ • 0x17ca4:$s6: SOFTWARE\RealVNC\ • 0x17cd0:$s6: SOFTWARE\RealVNC\ • 0x18008:$s7: SOFTWARE\TightVNC\ • 0x18034:$s7: SOFTWARE\TightVNC\ • 0x18060:$s7: SOFTWARE\TightVNC\ • 0x180ac:$s7: SOFTWARE\TightVNC\ • 0x1c43c:$s8: cred.dll
C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll	INDICATOR_TOOL_PWS_Amady	Detects password stealer DLL. Dropped by Amadey	ditekSHen	• 0xd868:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x15604:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x16074:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x15158:$s2: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook • 0x151bc:$s2: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook • 0xdd0c:$s3: \Mikrotik\Winbox\Addresses.cdb • 0x190d8:$s4: \HostName • 0x19100:$s5: \Password • 0x17c04:$s6: SOFTWARE\RealVNC\ • 0x17c30:$s6: SOFTWARE\RealVNC\ • 0x17c5c:$s6: SOFTWARE\RealVNC\ • 0x17ca4:$s6: SOFTWARE\RealVNC\ • 0x17cd0:$s6: SOFTWARE\RealVNC\ • 0x18008:$s7: SOFTWARE\TightVNC\ • 0x18034:$s7: SOFTWARE\TightVNC\ • 0x18060:$s7: SOFTWARE\TightVNC\ • 0x180ac:$s7: SOFTWARE\TightVNC\ • 0x1c43c:$s8: cred.dll
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
0000001D.00000000.425029230.0000000000F01000.00000020.00000001.01000000.0000000D.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
0000001D.00000002.428729367.0000000000F01000.00000020.00000001.01000000.0000000D.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
0000000E.00000000.403627141.0000000000DD1000.00000020.00000001.01000000.0000000A.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
00000015.00000003.498981390.0000000000C04000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Amadey	Yara detected Amadey bot	Joe Security	
0000002B.00000003.588957160.0000000000490000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 51 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
43.3.thgcici.490000.0.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
14.0.9545.exe.dd0000.0.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
11.2.thgcici.6a0e67.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
44.2.gntuud.exe.f00000.0.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
14.0.9545.exe.dd0000.3.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
Click to see the 20 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949801802027700 12/13/22-20:09:37.904526
SID:	2027700
Source Port:	49801
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949764802027700 12/13/22-20:09:24.415498
SID:	2027700
Source Port:	49764
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949749802027700 12/13/22-20:09:18.397632
SID:	2027700
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949767802027700 12/13/22-20:09:25.222687
SID:	2027700
Source Port:	49767
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949795802027700 12/13/22-20:09:35.735518
SID:	2027700
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949770802027700 12/13/22-20:09:26.190276
SID:	2027700
Source Port:	49770
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.3 - Destination IP: 185.246.221.151	
Timestamp:	192.168.2.3185.246.221.15149699802851815 12/13/22-20:08:50.072694
SID:	2851815
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949740802027700 12/13/22-20:09:15.487438

SID:	2027700
Source Port:	49740
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949798802027700 12/13/22-20:09:36.748511
SID:	2027700
Source Port:	49798
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949746802027700 12/13/22-20:09:17.426965
SID:	2027700
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949743802027700 12/13/22-20:09:16.449856
SID:	2027700
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949761802027700 12/13/22-20:09:23.806620
SID:	2027700
Source Port:	49761
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949752802027700 12/13/22-20:09:21.874851
SID:	2027700
Source Port:	49752
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949771802027700 12/13/22-20:09:26.565033
SID:	2027700
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949802802027700 12/13/22-20:09:39.191576
SID:	2027700
Source Port:	49802
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949748802027700 12/13/22-20:09:18.100262
SID:	2027700
Source Port:	49748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949777802027700 12/13/22-20:09:30.589327
SID:	2027700
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949742802027700 12/13/22-20:09:16.147180
SID:	2027700
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949794802027700 12/13/22-20:09:35.428306
SID:	2027700
Source Port:	49794
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949789802027700 12/13/22-20:09:34.068418
SID:	2027700
Source Port:	49789
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949754802027700 12/13/22-20:09:22.487126
SID:	2027700
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949782802027700 12/13/22-20:09:32.020133
SID:	2027700
Source Port:	49782
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949747802027700 12/13/22-20:09:17.691856

SID:	2027700
Source Port:	49747
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949760802027700 12/13/22-20:09:23.551005
SID:	2027700
Source Port:	49760
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949776802027700 12/13/22-20:09:30.348436
SID:	2027700
Source Port:	49776
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949753802027700 12/13/22-20:09:22.159892
SID:	2027700
Source Port:	49753
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949759802027700 12/13/22-20:09:23.268020
SID:	2027700
Source Port:	49759
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949783802027700 12/13/22-20:09:32.395745
SID:	2027700
Source Port:	49783
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949807802027700 12/13/22-20:09:40.738951
SID:	2027700
Source Port:	49807
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949788802027700 12/13/22-20:09:33.792525
SID:	2027700
Source Port:	49788
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949765802027700 12/13/22-20:09:24.668106
SID:	2027700
Source Port:	49765
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949787802027700 12/13/22-20:09:33.525784
SID:	2027700
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949790802027700 12/13/22-20:09:34.337562
SID:	2027700
Source Port:	49790
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949796802027700 12/13/22-20:09:36.034730
SID:	2027700
Source Port:	49796
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949781802027700 12/13/22-20:09:31.753391
SID:	2027700
Source Port:	49781
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949772802027700 12/13/22-20:09:29.469495
SID:	2027700
Source Port:	49772
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949735802027700 12/13/22-20:09:14.280167
SID:	2027700
Source Port:	49735
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949741802027700 12/13/22-20:09:15.797540

SID:	2027700
Source Port:	49741
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949799802027700 12/13/22-20:09:37.255404
SID:	2027700
Source Port:	49799
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949766802027700 12/13/22-20:09:24.922545
SID:	2027700
Source Port:	49766
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949803802027700 12/13/22-20:09:39.585529
SID:	2027700
Source Port:	49803
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949806802027700 12/13/22-20:09:40.381114
SID:	2027700
Source Port:	49806
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949757802027700 12/13/22-20:09:23.006710
SID:	2027700
Source Port:	49757
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949778802027700 12/13/22-20:09:30.907345
SID:	2027700
Source Port:	49778
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	▬
Timestamp:	192.168.2.362.204.41.7949775802027700 12/13/22-20:09:30.081643
SID:	2027700
Source Port:	49775
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949793802027700 12/13/22-20:09:35.174611
SID:	2027700
Source Port:	49793
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949800802027700 12/13/22-20:09:37.581033
SID:	2027700
Source Port:	49800
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949784802027700 12/13/22-20:09:32.706051
SID:	2027700
Source Port:	49784
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949769802027700 12/13/22-20:09:25.868942
SID:	2027700
Source Port:	49769
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949774802027700 12/13/22-20:09:29.736811
SID:	2027700
Source Port:	49774
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949805802027700 12/13/22-20:09:40.125674
SID:	2027700
Source Port:	49805
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949768802027700 12/13/22-20:09:25.563234
SID:	2027700
Source Port:	49768
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949751802027700 12/13/22-20:09:20.733567

SID:	2027700
Source Port:	49751
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79

Timestamp:	192.168.2.362.204.41.7949786802027700 12/13/22-20:09:33.253065
SID:	2027700
Source Port:	49786
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79

Timestamp:	192.168.2.362.204.41.7949791802027700 12/13/22-20:09:34.581849
SID:	2027700
Source Port:	49791
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79

Timestamp:	192.168.2.362.204.41.7949739802027700 12/13/22-20:09:15.157831
SID:	2027700
Source Port:	49739
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79

Timestamp:	192.168.2.362.204.41.7949745802027700 12/13/22-20:09:17.106517
SID:	2027700
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79

Timestamp:	192.168.2.362.204.41.7949750802027700 12/13/22-20:09:19.302564
SID:	2027700
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79

Timestamp:	192.168.2.362.204.41.7949792802027700 12/13/22-20:09:34.882839
SID:	2027700
Source Port:	49792
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79

Timestamp:	192.168.2.362.204.41.7949779802027700 12/13/22-20:09:31.163445
SID:	2027700
Source Port:	49779
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949785802027700 12/13/22-20:09:32.996655
SID:	2027700
Source Port:	49785
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949744802027700 12/13/22-20:09:16.793275
SID:	2027700
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949780802027700 12/13/22-20:09:31.434688
SID:	2027700
Source Port:	49780
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949738802027700 12/13/22-20:09:14.724261
SID:	2027700
Source Port:	49738
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949762802027700 12/13/22-20:09:24.088211
SID:	2027700
Source Port:	49762
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949804802027700 12/13/22-20:09:39.864342
SID:	2027700
Source Port:	49804
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949756802027700 12/13/22-20:09:22.763314
SID:	2027700
Source Port:	49756
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 62.204.41.79	
Timestamp:	192.168.2.362.204.41.7949797802027700 12/13/22-20:09:36.311423

SID:	2027700
Source Port:	49797
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected SmokeLoader

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (changes PE section rights)

Persistence and Installation Behavior

Yara detected Amadey bot

Boot Survival

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

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

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

Malware Analysis System Evasion

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

HIPS / PFW / Operating System Protection Evasion

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

Benign windows process drops PE files

Maps a DLL or memory area into another process

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

Injects code into the Windows Explorer (explorer.exe)

Stealing of Sensitive Information

Yara detected Amadeys stealer DLL

Yara detected SmokeLoader

Yara detected Amadey bot

Yara detected Vidar stealer

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

Tries to steal Instant Messenger accounts or passwords

Remote Access Functionality

Yara detected SmokeLoader

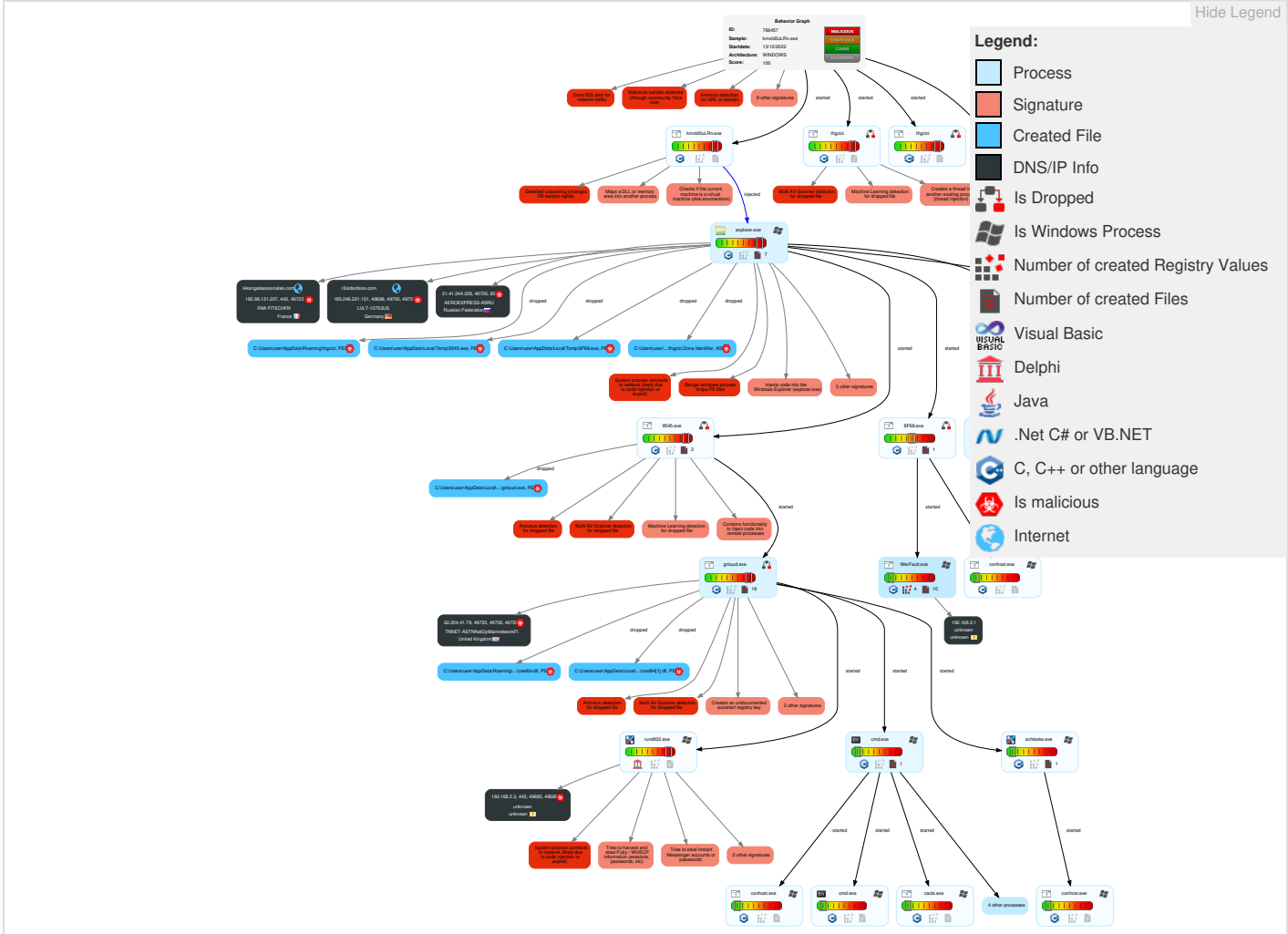
Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Exploitation for Client Execution	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	1 DLL Side-Loading	2 Obfuscated Files or Information	1 Input Capture	1 Account Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	1 Registry Run Keys / Startup Folder	6 1 2 Process Injection	1 1 Software Packing	2 Credentials in Registry	2 File and Directory Discovery	SMB/Windows Admin Shares	1 Screen Capture	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	1 Services File Permissions Weakness	1 Scheduled Task/Job	1 DLL Side-Loading	1 Credentials In Files	3 5 System Information Discovery	Distributed Component Object Model	1 Email Collection	Scheduled Transfer	1 2 5 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 Registry Run Keys / Startup Folder	1 File Deletion	LSA Secrets	2 3 1 Security Software Discovery	SSH	1 Input Capture	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	1 Services File Permissions Weakness	1 1 Masquerading	Cached Domain Credentials	2 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 1 Virtualization/Sandbox Evasion	DCSync	3 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	6 1 2 Process Injection	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Services File Permissions Weakness	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Rundll32	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

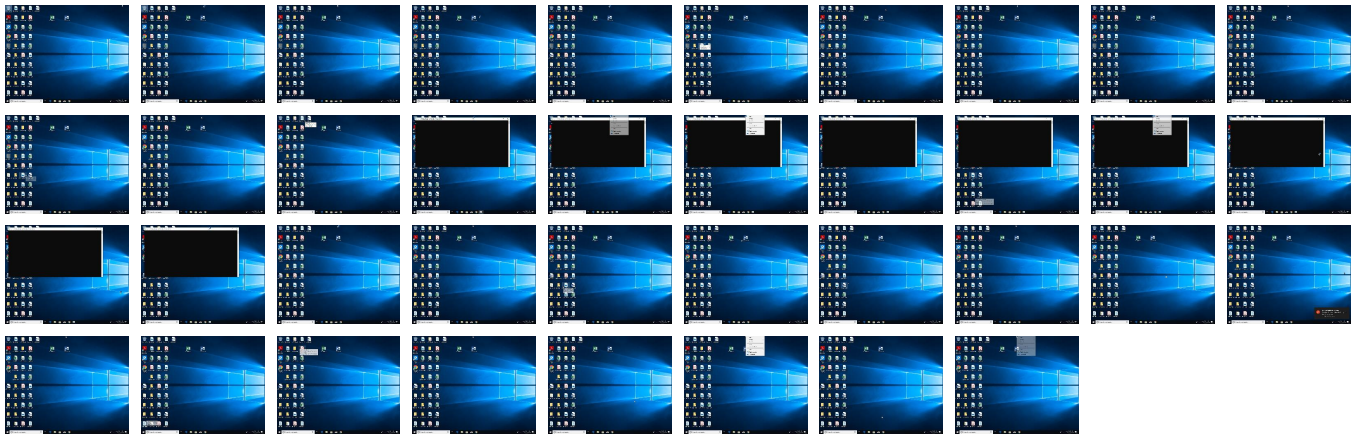
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
kmxId0uLRn.exe	69%	ReversingLabs	Win32.Trojan.Raccoon	
kmxId0uLRn.exe	60%	Virustotal		Browse
kmxId0uLRn.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	100%	Avira	HEUR/AGEN.1233121	
C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe	100%	Avira	HEUR/AGEN.1253146	
C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll	100%	Avira	HEUR/AGEN.1233121	
C:\Users\user\AppData\Local\Temp\9545.exe	100%	Avira	HEUR/AGEN.1253146	
C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8F68.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\9545.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\thgcici	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	79%	ReversingLabs	Win32.Infostealer.Decred	
C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe	53%	ReversingLabs	Win32.Trojan.Lazy	
C:\Users\user\AppData\Local\Temp\9545.exe	53%	ReversingLabs	Win32.Trojan.Lazy	
C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll	79%	ReversingLabs	Win32.Infostealer.Decred	
C:\Users\user\AppData\Roaming\thgcici	69%	ReversingLabs	Win32.Trojan.Raccoon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
43.2.thgcici.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.3.thgcici.2090000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.9545.exe.dd0000.3.unpack	100%	Avira	HEUR/AGEN.1253146		Download File
44.0.gntuud.exe.f00000.0.unpack	100%	Avira	HEUR/AGEN.1253146		Download File
29.2.gntuud.exe.f00000.0.unpack	100%	Avira	HEUR/AGEN.1253146		Download File
12.0.8F68.exe.c42a60.7.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.0.9545.exe.dd0000.0.unpack	100%	Avira	HEUR/AGEN.1253146		Download File
11.2.thgcici.6a0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.9545.exe.dd0000.2.unpack	100%	Avira	HEUR/AGEN.1253146		Download File
44.2.gntuud.exe.f00000.0.unpack	100%	Avira	HEUR/AGEN.1253146		Download File
12.2.8F68.exe.c42a60.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.9545.exe.dd0000.0.unpack	100%	Avira	HEUR/AGEN.1253146		Download File
12.0.8F68.exe.c42a60.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
21.2.gntuud.exe.f00000.0.unpack	100%	Avira	HEUR/AGEN.1253146		Download File
14.0.9545.exe.dd0000.1.unpack	100%	Avira	HEUR/AGEN.1253146		Download File
21.0.gntuud.exe.f00000.0.unpack	100%	Avira	HEUR/AGEN.1253146		Download File
0.3.kmxId0uLRn.exe.5e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.thgcici.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.kmxId0uLRn.exe.5d0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
43.3.thgcici.490000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
43.2.thgcici.470e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.0.gntuud.exe.f00000.0.unpack	100%	Avira	HEUR/AGEN.1253146		Download File
0.2.kmxId0uLRn.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
r3oidsofsios.com	3%	Virustotal		Browse
kikangalaassociates.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
62.204.41.79/fb73jc3/index.php	0%	Avira URL Cloud	safe	
http://62.204.41.79/fb73jc3/index.php?scr=1t&	0%	Avira URL Cloud	safe	
http://62.204.41.79/fb73jc3/index.php?scr=1	0%	Avira URL Cloud	safe	
http://62.204.41.79/fb73jc3/index.php?scr=1l&	0%	Avira URL Cloud	safe	
http://62.204.41.79/fb73jc3/Plugins/cred64.dll	100%	Avira URL Cloud	malware	
http://62.204.41.79/fb73jc3/index.phpa	0%	Avira URL Cloud	safe	
http://62.204.41.79/fb73jc3/index.phpg	0%	Avira URL Cloud	safe	
http://62.204.41.79/fb73jc3/index.php?scr=1T)	0%	Avira URL Cloud	safe	
http://62.204.41.79/fb73jc3/index.phpM	0%	Avira URL Cloud	safe	
http://62.204.41.79/fb	0%	Avira URL Cloud	safe	
http://62.204.41.79/fb73jc3/index.phpcu	0%	Avira URL Cloud	safe	
http://62.204.41.79/fb73jc3/Plugins/cred64.dllXIK	0%	Avira URL Cloud	safe	
http://62.204.41.79/fbfb73jc3/index.php	0%	Avira URL Cloud	safe	
http://62.204.41.79/fb73jc3/index.php	0%	Avira URL Cloud	safe	
http://62.204.41.79/fb73jc3/index.phpwu$	0%	Avira URL Cloud	safe	
http://62.204.41.79/fb73jc3/index.phpqu.	0%	Avira URL Cloud	safe	
http://https://kikangalaassociates.com/vidar2.exe	0%	Avira URL Cloud	safe	
http://s2scomm20.com/	100%	Avira URL Cloud	malware	
http://c2csosi228d.com/	100%	Avira URL Cloud	malware	
http://31.41.244.228/fusa/bibar.exe	100%	Avira URL Cloud	malware	
http://95.217.27.105:80	0%	Avira URL Cloud	safe	
http://xdd42sdfsdf.com/	100%	Avira URL Cloud	malware	
http://r3oidsofsios.com/Mozilla/5.0	0%	Avira URL Cloud	safe	
http://62.204.41.79/fb73jc3/index.phpF	0%	Avira URL Cloud	safe	
http://r3oidsofsios.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
r3oidsofsios.com	185.246.221.151	true	true	• 3%, Virustotal, Browse	unknown
kikangalaassociates.com	185.98.131.207	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://steamcommunity.com/profiles/76561199443972360	false		high
62.204.41.79/fb73jc3/index.php	true	• Avira URL Cloud: safe	low
http://62.204.41.79/fb73jc3/index.php?scr=1	true	• Avira URL Cloud: safe	unknown

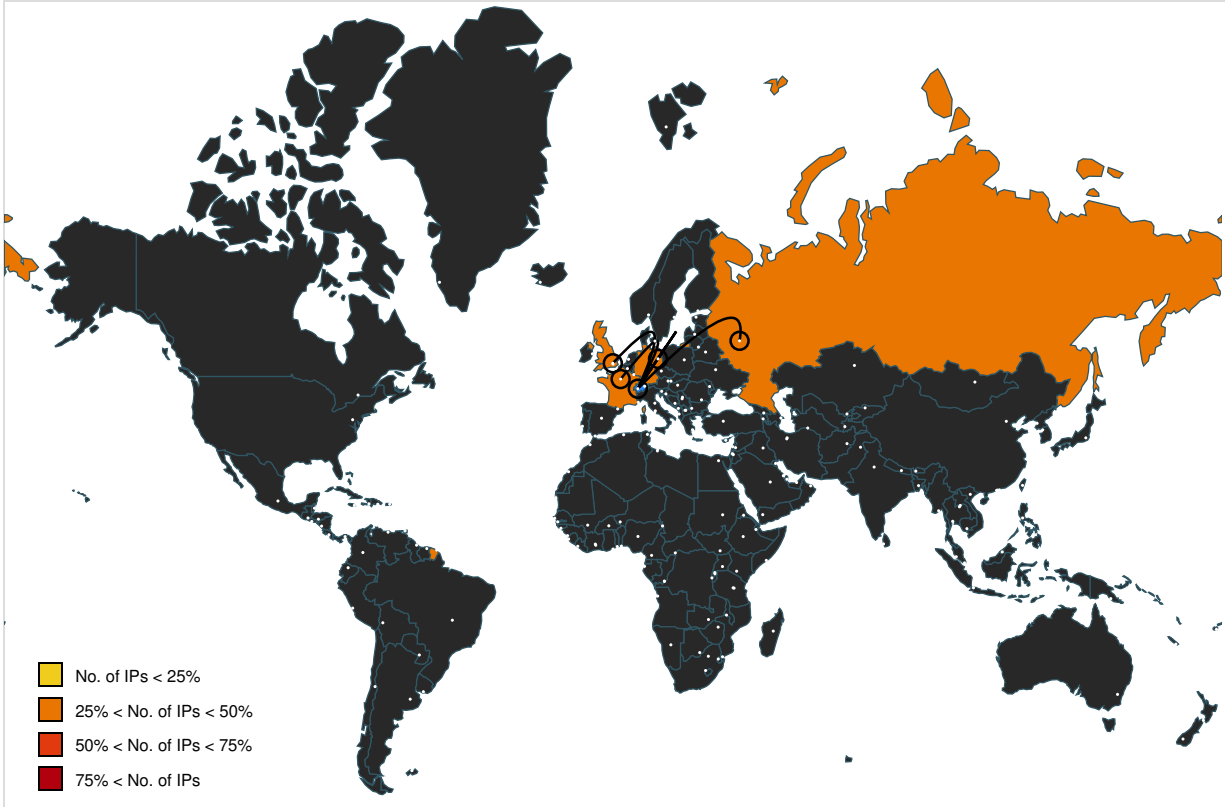
Name	Malicious	Antivirus Detection	Reputation
http://https://kikangalaassociates.com/vidar2.exe	false	• Avira URL Cloud: safe	unknown
http://62.204.41.79/fb73jc3/Plugins/cred64.dll	true	• Avira URL Cloud: malware	unknown
http://31.41.244.228/fusa/bibar.exe	true	• Avira URL Cloud: malware	unknown
http://c2csosi228d.com/	true	• Avira URL Cloud: malware	unknown
http://s2scomm20.com/	true	• Avira URL Cloud: malware	unknown
http://62.204.41.79/fb73jc3/index.php	true	• Avira URL Cloud: safe	unknown
http://https://t.me/ttruelive	false		high
http://xdd42sdfsdf.com/	true	• Avira URL Cloud: malware	unknown
http://r3oidsofsios.com/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://62.204.41.79/fb73jc3/index.php?scr=1t&	gntuud.exe, 00000015.00000002.787565484.0000000000C39000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.google.com/search	explorer.exe, 0000001F.00000002.776413883.0000000003441000.00000040.80000000.00040000.00000000.sdmp	false		high
http://62.204.41.79/fb73jc3/index.php?scr=1l&	gntuud.exe, 00000015.00000003.499244475.0000000000C39000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://go.mail.ru/search	explorer.exe, 0000001F.00000002.776413883.0000000003441000.00000040.80000000.00040000.00000000.sdmp	false		high
http://62.204.41.79/fb73jc3/index.phpa	gntuud.exe, 00000015.00000002.785290818.0000000000BF4000.00000004.00000020.00020000.00000000.sdmp, gntuud.exe, 00000015.00000003.499661889.0000000000BF4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nova.rambler.ru/search	explorer.exe, 0000001F.00000002.776413883.0000000003441000.00000040.80000000.00040000.00000000.sdmp	false		high
http://62.204.41.79/fb	gntuud.exe, 00000015.00000003.499113255.0000000000C1F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://62.204.41.79/fb73jc3/index.phpg	gntuud.exe, 00000015.00000003.499037932.0000000000C14000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t.me/ttruelivehttps://steamcommunity.com/profiles/76561199443972360 95.217.27.105:80hi	8F68.exe, 0000000C.00000000.404562471.0000000000C42000.00000004.00000001.01000000.00000009.sdmp	false		high
http://search.yahoo.com/search	explorer.exe, 0000001F.00000002.776413883.0000000003441000.00000040.80000000.00040000.00000000.sdmp	false		high
http://62.204.41.79/fb73jc3/index.php?scr=1T)	gntuud.exe, 00000015.00000002.787565484.0000000000C39000.00000004.00000020.00020000.00000000.sdmp, gntuud.exe, 00000015.00000003.499244475.0000000000C39000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://62.204.41.79/fb73jc3/index.phpcu	gntuud.exe, 00000015.00000002.786384130.0000000000C14000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.aol.com/aol/search	explorer.exe, 0000001F.00000002.776413883.0000000003441000.00000040.80000000.00040000.00000000.sdmp	false		high
http://62.204.41.79/fb73jc3/index.phpM	gntuud.exe, 00000015.00000002.786658213.0000000000C1D000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://62.204.41.79/fbfb73jc3/index.php	gntuud.exe, 00000015.00000002.786658213.0000000000C1D000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://62.204.41.79/fb73jc3/Plugins/cred64.dllXIK	gntuud.exe, 00000015.00000003.498981390.0000000000C04000.00000004.00000020.00020000.00000000.sdmp, gntuud.exe, 00000015.00000002.785970616.0000000000C07000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://62.204.41.79/fb73jc3/index.phpqu.	gntuud.exe, 00000015.00000003.499037932.0000000000C14000.00000004.00000020.00020000.00000000.sdmp, gntuud.exe, 00000015.00000002.786384130.0000000000C14000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://62.204.41.79/fb73jc3/index.phpwu$	gntuud.exe, 00000015.00000003.499037932.0000000000C14000.00000004.00000020.00020000.00000000.sdmp, gntuud.exe, 00000015.00000002.786384130.0000000000C14000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3oidsofsios.com/Mozilla/5.0	explorer.exe, 00000011.00000000.405174014.00000000004F0000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 00000012.00000002.775161398.0000000001090000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000012.00000000.413703435.0000000000EE0000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 00000013.00000002.779312783.000000000B57000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000013.00000000.417309353.0000000000530000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 00000016.00000002.775858605.00000000006D8000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.420551387.00000000006C0000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 0000001A.00000002.780502207.000000003377000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001F.00000000.426593885.0000000003450000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 00000022.00000000.429438818.00000000005F0000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 00000026.00000002.777038253.0000000000650000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000028.00000000.435504290.0000000000530000.00000040.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://95.217.27.105:80	8F68.exe, 0000000C.00000000.404562471.000000000C42000.00000004.00000001.01000000.00000009.sdmp	false	• Avira URL Cloud: safe	unknown
http://62.204.41.79/fb73jc3/index.phpF	gntuud.exe, 00000015.00000003.499113255.0000000000C1F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.41.244.228	unknown	Russian Federation		61974	AEROEXPRESS-ASRU	true
185.246.221.151	r3oidsofsios.com	Germany		10753	LVLT-10753US	true
62.204.41.79	unknown	United Kingdom		30798	TNNET-ASTNNetOyMainnetworkFI	true
185.98.131.207	kikangalaassociates.com	France		16347	RMI-FITECHFR	true

Private

IP
192.168.2.1
192.168.2.3

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	766457
Start date and time:	2022-12-13 20:06:50 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	kmxId0uLRn.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	46
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.phis.troj.spyw.evad.winEXE@51/18@28/6
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 60.2% (good quality ratio 54.3%) • Quality average: 71.8% • Quality standard deviation: 32.3%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for rundll32

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.42.73.29
- Excluded domains from analysis (whitelisted): fs.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:08:51	Task Scheduler	Run new task: Firefox Default Browser Agent 4D11EF12B087A959 path: C:\Users\user\AppData\Roaming\thg cici
20:09:07	Task Scheduler	Run new task: gntuud.exe path: C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe
20:09:07	API Interceptor	1283x Sleep call for process: explorer.exe modified
20:09:07	API Interceptor	1401x Sleep call for process: gntuud.exe modified
20:09:15	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_8F68.exe_a1299b47a4636d69dc3bf7715d1130fd3baa11_d5638d9e_08cf2d1b\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6772632143876667
Encrypted:	false
SSDEEP:	96:YI7FpFaefLzFhBX7kRC6tpXIQcQvc6QcEDMcw3Db+HbHg/8BRTf3OyWZAXGng5FA:YRjFaUsHBUZMXYjuq/u7sqS274ItL7
MD5:	3B1C322E839ACACBA456FEDD9F393D9E
SHA1:	1901D98FC6CC533884C755A93835ACD0B683EE47
SHA-256:	D21A2F3BDE2CDB1E09E849A1953EAB93FC493182E98400C910AED2C54FD563B8
SHA-512:	5C9335AE5292820E5E5B73C28C869B3B9134080D2E2CAA2368816A02B46C21C1BE0D2FA43C713ED610AF1A34376B3C2415E9B376FEDD1217E670EE0A32EA667C
Malicious:	false
Reputation:	unknown

Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.1.5.4.6.4.5.4.4.2.9.1.1.0.1.8.....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.=.1.3.3.1.5.4.6.4.5.4.6.7.9.1.0.9.3.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.3.0.8.9.e.4.6.-.b.1.6.0.-.4.1.a.6.-.9.8.3.4.-.b.5.2.2.1.c.e.d.e.6.a.3.....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.=.d.4.4.5.c.e.2.e.-.2.c.5.d.-.4.8.0.4.-.b.4.a.f.-.f.d.0.5.1.0.0.b.e.d.c.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.8.F.6.8...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.6.2.0.-.0.0.0.1.-.0.0.1.f.-.5.c.7.5.-.7.c.c.8.7.1.0.f.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.2.3.f.0.1.9.6.9.b.2.7.5.4.4.4.2.2.2.3.b.5.1.b.f.7.8.e.5.d.4.4.6.0.0.0.0.f.f.f.f.!.0.0.0.0.8.e.b.0.c.7.d.0.2.f.c.8.a.a.6.b.6.c.5.a.7.c.7.1.e.a.6.0.b.c.3.3.3.a.a.3.d.1.c.7.!.8.F.6.8...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././.1.2././.1.3.:.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Dec 14 04:09:04 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	34894
Entropy (8bit):	2.098097190395399
Encrypted:	false
SSDEEP:	192:u2A9k2HFvOth7eZ1S6SRlmaRANO/4a08SdRLOEn:uZIthKD+4alMLOE
MD5:	57BB9A19DFFC3A30720BD4BC392CE63C
SHA1:	2841C2A5A4CA55248BAA12B03DDF45BF9A5E8080
SHA-256:	3B979F47F4E4CE93C4274A6ECB56FDD788156D662386482A1F7EB013B8A242B7
SHA-512:	27DADBE48BFE5F551A66C6A4B043ED16E33DB3272945BC36066DA3C0E54B32B393E9C0414A95DAAA8F5AF2234F02FE2539B51A9E71620F88A108659B68FB5ED2
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....`L.c.....$.....T.....8.....T.....v}.....U.....B.....4.....GenuineIntelW.....T..... ...WL.c..... .....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8332
Entropy (8bit):	3.6908615623175716
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi7+6z6YqJSUfDJgmfESP2Cpr389b+6sfSF9Km:RrlsNiy6z6Y0SU7JgmfESe+Zf0
MD5:	8C75001433EBA8F2FC9FF9E7B4184A9F
SHA1:	93424EAB7389399AAD4E1A19658AABA8E57920DC
SHA-256:	CC6E0DAD83E7E690B1490D293A1F41A66650FC633E2D4F708C92EF1CC87AA0D4
SHA-512:	E31F4013818DC7E9A48D35C069F90F295DD71D7E800497646FB7C9986AF3520B8DA78BB13251CA12116964CC0116021E1B9EB109867E4692098695B4F117C5E6
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.1.5.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER92B2.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4622
Entropy (8bit):	4.413835149815752
Encrypted:	false
SSDEEP:	48:cvIwSD8zseJgtWI951Wgc8sqYj88fm8M4JHMYUFgq+q8vYMYiGxMzjzOd:ulTfUSEgrsqYFJHncKYnnxKvOd
MD5:	8DDA398B6D27443E0F36BC858939DB98
SHA1:	91A75DE7B4D7A847C5056214FA0AEA7BEF84C419
SHA-256:	0136FD997E5CD393648033FFD1BCC76C162A7D76F210793D86695378D1EFDC7D
SHA-512:	36ED0CF0B4F0B0F61A200A499F2F28EEBDDB7BC42A91CC8D6FBA9CF59C568F11B9C3BDEECECD357FAEDE69161FEE9C5D1FD919D7AE8DE72C5CB1E8491AE82964
Malicious:	false
Reputation:	unknown

Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1822399" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

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

Process:	C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	129024
Entropy (8bit):	6.511616263388435
Encrypted:	false
SSDEEP:	3072:ox7pOYzBekcmWDWCMq6As523HeS9FAiZ87vO2rlL3Rne9:ox7ZNhc/dMq6AO0a7vVIT
MD5:	9995ABF2F401E4945A7D2930A3727619
SHA1:	7715E14AD6E4ADF609C62C5812419800343FBD4F
SHA-256:	D35B5DD18D91DBFE3DC89CB75B6A26757777B5C52A33CD8FCF6E5ED45A946F1A
SHA-512:	42726FB602958594914B5BC936AFF36833823F9F9DA9BC80A46579D96CEC12C7DF070C174EC9DD82C21F2FE44F1E9A4A2E50D9944FEA6379DBDEC666727A7EE A
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll, Author: Joe Security • Rule: INDICATOR_TOOL_PWS_Amady, Description: Detects password stealer DLL. Dropped by Amadey, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 79%
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....X.....x.....@.....@.....O.....&.... ....CODE..... ..`DATA.....@...BSS.....idata..&.....@....edata..O.....@..P.reloc .....@..P.rsrc..... .....@..P.....@.....@..P..... .....

C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe

Process:	C:\Users\user\AppData\Local\Temp\9545.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	249344
Entropy (8bit):	6.371571449774557
Encrypted:	false
SSDEEP:	6144:90Tn/MUTehRBZbSjpwe6N+6LzXFuz5a6EKhK6Kr3ZpO:yXg7Zb46FLBuz5aD46zO
MD5:	C6524CC2CB091E23BE6D9526D6BCBC99
SHA1:	8A1FC0333392DCD9FF664F64CE88D7ABDFD882DC
SHA-256:	37DE71B43236C63687B44F238A17CDE5F16BEA2B2EC8C29B0EA42B62DE947D6D
SHA-512:	FA7CEE2EBC9A445830505C078DBD870D809E1F829B202E75A6CE7C8BB728CE7CC68D6980EE0989FD6EE9DEF2DAA0C4EB67D8A462EB4F8583B20760FFC8DF1 3C6
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 53%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....XH..6...6...6...5...6...3.a.6...2...6.(.2...6.(.5...6.(.3...6...7...6...7.\.6.f. ?...6.f.....6.f.4...6.Rich..6.....PE..L.....c.....@.....@.....0.....@.....P)..._..p..... ..@.....\.....text...v..... ..`.rdata..D.....@..@.data...LD.....@....rsrc.....@..@.reloc..P).....*..... .....@..B..... .....

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

Process:	C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, components 3
Category:	dropped
Size (bytes):	105976
Entropy (8bit):	7.9288617581895435

Encrypted:	false
SSDEEP:	1536:CYwlbiXP6ZT2fSPHA04D+fcBB0YugBbgaMiKmXaljqZ73TCn1R73exu+jA9Ops8u:bwRiCpC+A04qcX0YfXVOxMtNFnSop
MD5:	AF9EDCF2AE7CA1F5DF3AB8FAEE735473
SHA1:	06218105DAA6BF86C04F0937C634E3C2C6B75A71
SHA-256:	02B2FE6FE005D6A31AABAC0E69BB44689B5F3918FBFB45A36BCE9E5838787FE8
SHA-512:	7F95A873B775494543F807A8CB0A4E29A0590235AC747D839EA3E0AB0322A8AC63E343040155999CFC7D9FF345456F4EF73CC84C650BDC4F825A75F160EF9227
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`.....C.................................. $.' ",#..(7),01444.'9=82<.342...C..........2!.!22222222222222222222222222222222222222222222222222..........".................. ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....?..01KK...lq\....xcS.m..#Hm.....T......<!...wq5...v1.?S.....rHj-.U:...5...........|..+.......}...<.>...H.......Wo.CK`/l.1./...C...W.....,1....R.0.W......qco;.\..%r........H.'.|..)..m..e#.. N.}5y._.pY\L.w[....r....%.......5...L..S....CN5b..6..>.... ZJ(......x+...4.../..[.#(b.NFs.Vu*F.y..*1rvG.K^.>._.?.....?.U..n...D>......g.a...F..U.#.h...>...Q...]...m...

C:\Users\user\AppData\Local\Temp\8F68.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	559616
Entropy (8bit):	7.300452125448157
Encrypted:	false
SSDEEP:	12288:9Q43DNbQ6lAwyJLiAM/K+M11HTbcxk48KAGoX81Ca:9lbByJLijK+M19N48KZv
MD5:	46F30465FA693033E7D3D78468406C0C
SHA1:	8EB0C7D02FC8AA6B6C5A7C71EA60BC333AA3D1C7
SHA-256:	3775F0AA5B9D87F0237FF1249F5E8548EBA54F23EABCF62C199564E0966662E4
SHA-512:	CF6680239B2D94E5D878E3902D9368B6B52675C1A8C0C780B4F5737BADA268A4A954C15655039364F68B6081DCFC325C103DB03EB49521438987C75D415B1F24
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.........;.cU..cU..cU...V..cU...P..cU...Q..cU...Q..cU...V..cU...T..cU ..cT..cU...P..cU...\..cU......cU...W..cU.Rich.cU................PE..L......c.............. ."...r......It.......@....@.......................................@....................................<...............................4 ... .`...@...........@..8...........................text....!......."................. ..`.rdata.......@.......&.............@..@.data...px... ...l.................@....rsrc...............l..... ....@..@.reloc..4...........n.............@..B.. ....

C:\Users\user\AppData\Local\Temp\9545.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	249344
Entropy (8bit):	6.371571449774557
Encrypted:	false
SSDEEP:	6144:90Tn/MUTehRBZbSjpwe6N+6LzXFuz5a6EKhK6Kr3ZpO:yXg7Zb46FLBuz5aD46zO
MD5:	C6524CC2CB091E23BE6D9526D6BCBC99
SHA1:	8A1FC0333392DCD9FF664F64CE88D7ABDFD882DC
SHA-256:	37DE71B43236C63687B44F238A17CDE5F16BEA2B2EC8C29B0EA42B62DE947D6D
SHA-512:	FA7CEE2EBC9A445830505C078DBD870D809E1F829B202E75A6CE7C8BB728CE7CC68D6980EE0989FD6EE9DEF2DAA0C4EB67D8A462EB4F8583B20760FFC8DF 3C6
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Temp\9545.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 53%
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.........XH..6...6...6...5...6...3.a.6...2...6.(.2...6.(.5...6.(.3...6...7...6...7.\.6.f. ?...6.f.....6.f.4...6.Rich..6.........PE..L......c...........................@............@.........................0............@..P)..._..p..........................._ ..@..............\...........................text...v.......................... ..`.rdata..D..........................@..@.data...LD.........................@....rsrc..............................@..@.reloc..P).......*...... ....@..B.. ....

C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll

Process:	C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	129024
Entropy (8bit):	6.511616263388435
Encrypted:	false
SSDEEP:	3072:ox7pOYzBekcmWDWCMq6As523HeS9FAiZ87vO2rlL3Rne9:ox7ZNhc/dMq6AO0a7vVIT
MD5:	9995ABF2F401E4945A7D2930A3727619
SHA1:	7715E14AD6E4ADF609C62C5812419800343FBD4F
SHA-256:	D35B5DD18D91DBFE3DC89CB75B6A26757777B5C52A33CD8FCF6E5ED45A946F1A
SHA-512:	42726FB602958594914B5BC936AFF36833823F9F9DA9BC80A46579D96CEC12C7DF070C174EC9DD82C21F2FE44F1E9A4A2E50D9944FEA6379DBDEC666727A7EE A
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll, Author: Joe Security • Rule: INDICATOR_TOOL_PWS_Amady, Description: Detects password stealer DLL. Dropped by Amadey, Source: C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 79%
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....X.....x.....@.....@.....O.....&.... ....CODE..... ..`DATA.....@...BSS.....idata..&.....@....edata..O.....@..P.reloc .....@..P.rsrc..... .....@..P.....@.....@..P..... .....

C:\Users\user\AppData\Roaming\eubbvwb

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	160970
Entropy (8bit):	**7.998987236677346**
Encrypted:	**true**
SSDEEP:	3072:ryKvP/FpzgLSFlw8Tsl0+NNr5+7Vp3NW21IrUu6d3O9dk5OaSZIViIFX4Kp46Afj:rXPLzCSLjTslhB5+7VgUu6MdaSZsAFXI
MD5:	12924AF0CE2C960BE50DE7A77879C2CC
SHA1:	83281053BE86A582D1A6591F1E596E437E32FCDE
SHA-256:	689BFCDCFF48E4EC3FF5660CC03913B6F45DA0622E8325EF3F3D75AFD2E343B0
SHA-512:	A7A0FCE274538DA72428D53CFEB593E2AE88ED0420E4D83E18FFF3561C41C9E5210AD9AC5AD27270473E6BD03F182D62218BFC5CB842937A5C554AB486DF494
Malicious:	false
Reputation:	unknown
Preview:	.....[D..qU.. :.=.P...$.T.3.K..+...AUh....w....Utk.....i..{.nU.S|.;.X.....;.;?aS.!l.v....A..B....E%.cg.K.o....*.|.*@W.*...K...F.R*.&`.=.!.42<S..&..8..|.<....c....^....~.EG...IX..h...T..p... ;gQ%K0WW...x..H9..0.I%.m...K..=..k..r.N=.....n.H..Ko.QNP5.$O..H`lZ.W3..K.....#....'D..W2....V."......u.(B.^0.P.6,^'1)u(.T..".....u...F..V...+J.j..,yM.Q..Op.....cx.C..u.lh7.(..WFI. ...E.%..d..b.....;%S..... .Y.%.3..Ow.2T..q.@.|..!..v..f... .s..E..x.....`..b...tv.....*....'..X...Z..q#+.....*.@U.C{.....Mc.Q,...k!dv$E+8.....@..T.....97#.....PU.....3h.5*..* w....<<WQQ*.P.<.2.gO.....F...E.R..9e..G....z]...1....w....]...Mx,!.....r!...oY[w.....i|{Y.Bq.O....9.....W.-lS.....p. .Y...5d..@..r/Ug.....^.J...:.D...~...._.!..\...|._.~..x(..7$.,I).....i.p)..3..YI.3C....B?8:...T{..'...I:.'>#.;.:p.&..T....~...I.....Y....Q-V...@?..\.4..~.:h...u[.L....Y.w..q...x.O.....@.F..3....-.sKD.^....9.u.Wo..zW).....,...@.....:..\$.I.>....;._.

C:\Users\user\AppData\Roaming\thgcici

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	244736
Entropy (8bit):	6.678359541055903
Encrypted:	false
SSDEEP:	3072:0Rn60LZzxCCPaCK5T3cyT/KYtNMHO2R2NiruKiwNXJ2v40T2ui7lY6:mRL+CPaas/K02HOBNKnOv9T2lhY6
MD5:	C8782DA2928F63712D03D0EA36C57C3F
SHA1:	0D87BA5D17440501FE3629F56FEB0A9193D43B43
SHA-256:	A68B2D14B767DF5EDB784BC338C84E09D73AC90A75346A9FEDCE2B0163CA9656
SHA-512:	BDDF75CFBE80801F52CB4CAEBCA6E36569FABEBF99BB6AA702282B1E9423604D7C86A03CEE7F8FCA16A8DA521174530045E4C3CFACD34DE9306180B1D18291FF
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 69%
Reputation:	unknown

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....$./.`.A.`.A.`.A.~...u.A.~.....A.G.:.c.A.`.@...A.~...A.A.~...a.A.~...a.A.Rich`.A.....PE..L...N`.a.....".."...`.....=.....@....@.....$..(..... ..... (..@.....D.....text....!....."..... ..`.data...H....@.....&.....@....rsrc... .....2.....@..@..... ....

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

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

\Device\ConDrv

Process:	C:\Windows\SysWOW64\cacls.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	15
Entropy (8bit):	3.240223928941852
Encrypted:	false
SSDEEP:	3:o3F:o1
MD5:	509B054634B6DE74F111C3E646BC80FD
SHA1:	99B4C0F39144A92FE42E22473A2A2552FB16BD13
SHA-256:	07C7C151ADD6D955F3C876359C0E2A3A3FB0C519DD1E574413F0B68B345D8C36
SHA-512:	A9C2D23947DBE09D5ECFBF6B3109F3CF8409E43176AE10C18083446EDE006E60E41C3EA2D2765036A967FC81B085D5F271686606AED4154AE45287D412CF6D4
Malicious:	false
Reputation:	unknown
Preview:	processed dir:

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.678359541055903
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	kmxId0uLRn.exe
File size:	244736
MD5:	c8782da2928f63712d03d0ea36c57c3f
SHA1:	0d87ba5d17440501fe3629f56feb0a9193d43b43
SHA256:	a68b2d14b767df5edb784bc338c84e09d73ac90a75346a9fedce2b0163ca9656
SHA512:	bddf75cfbe80801f52cb4caebca6e36569fabebf99bb6aa702282b1e9423604d7c86a03cee7f8fca16a8da521174530045e4c3cfacd34de9306180b1d18291ff
SSDEEP:	3072:0Rn60LZzxCCPaCK5T3cyT/KYtNMHO2R2NiruKiwNXJ2v40T2ui7lY6:mRL+CPaas/K02HOBNKnOv9T2lhY6
TLSH:	DC34AD40BA93C462C291AD31CD69C6F1F739FDA599B6064F37187B3F6E303819622636
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....$./.`.A.`.A.`.A.~...u.A.~.....A.G.:.c.A.`.@...A.~...A.A.~...a.A.~...a.A.Rich`.A.....PE..L...N`.a.....".."...`.....

File Icon

Icon Hash:	beccae9eeea62aa2

Static PE Info

General

Entrypoint:	0x403df6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x611E604E [Thu Aug 19 13:44:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	e4727ec893dc979e33dd56cc7774fb31

Entrypoint Preview

Instruction
call 00007FF59867C275h
jmp 00007FF598677A3Eh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov esi, ecx
mov byte ptr [esi+0Ch], 00000000h
test eax, eax
jne 00007FF598677C25h
call 00007FF59867A76Dh
mov dword ptr [esi+08h], eax
mov ecx, dword ptr [eax+6Ch]
mov dword ptr [esi], ecx
mov ecx, dword ptr [eax+68h]
mov dword ptr [esi+04h], ecx
mov ecx, dword ptr [esi]
cmp ecx, dword ptr [00424528h]
je 00007FF598677BD4h
mov ecx, dword ptr [00424444h]
test dword ptr [eax+70h], ecx
jne 00007FF598677BC9h
call 00007FF59867CC94h
mov dword ptr [esi], eax
mov eax, dword ptr [esi+04h]
cmp eax, dword ptr [00424348h]
je 00007FF598677BD8h
mov eax, dword ptr [esi+08h]
mov ecx, dword ptr [00424444h]
test dword ptr [eax+70h], ecx

Instruction
jne 00007FF598677BCAh
call 00007FF59867C508h
mov dword ptr [esi+04h], eax
mov eax, dword ptr [esi+08h]
test byte ptr [eax+70h], 00000002h
jne 00007FF598677BD6h
or dword ptr [eax+70h], 02h
mov byte ptr [esi+0Ch], 00000001h
jmp 00007FF598677BCCh
mov ecx, dword ptr [eax]
mov dword ptr [esi], ecx
mov eax, dword ptr [eax+04h]
mov dword ptr [esi+04h], eax
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
sub esp, 10h
push esi
push dword ptr [ebp+0Ch]
lea ecx, dword ptr [ebp-10h]
call 00007FF598677B2Ah
mov esi, dword ptr [ebp+08h]
movsx eax, byte ptr [esi]
push eax
call 00007FF59867CE37h
cmp eax, 65h
jmp 00007FF598677BCEh
inc esi
movzx eax, byte ptr [esi]
push eax
call 00007FF59867CCE5h
test eax, eax
pop ecx
jne 00007FF598677BB3h
movsx eax, byte ptr [esi]

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1248c	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x40000	0x18920	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1290	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2820	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x244	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x121c2	0x12200	False	0.526239224137931	data	6.287587198243143	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x14000	0x2bf48	0x10c00	False	0.9437383395522388	data	7.832296161196346	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x40000	0x18920	0x18a00	False	0.5258565989847716	data	5.47809790236992	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x56668	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0x56798	0xf0	Device independent bitmap graphic, 24 x 48 x 1, image size 0		
RT_CURSOR	0x56888	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_CURSOR	0x57960	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x40930	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x40ff8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x41560	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x42608	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x42ab0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x43358	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x43a20	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x43f88	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x45030	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x459b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x45e80	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x46728	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x48cd0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x49da8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Raeto-Romance	Switzerland
RT_ICON	0x4ac50	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Raeto-Romance	Switzerland
RT_ICON	0x4b4f8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Raeto-Romance	Switzerland
RT_ICON	0x4bbc0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Raeto-Romance	Switzerland
RT_ICON	0x4c128	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	Raeto-Romance	Switzerland
RT_ICON	0x4e6d0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Raeto-Romance	Switzerland

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4f778	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	Raeto-Romance	Switzerland
RT_ICON	0x50100	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Raeto-Romance	Switzerland
RT_ICON	0x505e0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x51488	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x51b50	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x520b8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x54660	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x55708	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x56090	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Raeto-Romance	Switzerland
RT_STRING	0x58370	0x1da	data	Raeto-Romance	Switzerland
RT_STRING	0x58550	0x150	data	Raeto-Romance	Switzerland
RT_STRING	0x586a0	0x27c	data	Raeto-Romance	Switzerland
RT_ACCELERATOR	0x565d8	0x90	data	Raeto-Romance	Switzerland
RT_ACCELERATOR	0x56560	0x78	data	Raeto-Romance	Switzerland
RT_GROUP_CURSOR	0x57930	0x30	data		
RT_GROUP_CURSOR	0x58208	0x14	data		
RT_GROUP_ICON	0x49d78	0x30	data	Raeto-Romance	Switzerland
RT_GROUP_ICON	0x45e20	0x5a	data	Raeto-Romance	Switzerland
RT_GROUP_ICON	0x50568	0x76	data	Raeto-Romance	Switzerland
RT_GROUP_ICON	0x42a70	0x3e	data	Raeto-Romance	Switzerland
RT_GROUP_ICON	0x564f8	0x68	data	Raeto-Romance	Switzerland
RT_VERSION	0x58220	0x14c	Intel 80386 COFF executable, no relocation info, not stripped, 52 sections, symbol offset=0x5f0053, 4522070 symbols, optional header size 82, created Sat Mar 7 05:34:56 1970		

Imports

DLL	Import
KERNEL32.dll	LoadLibraryW, CallNamedPipeW, EnumSystemCodePagesW, EnumDateFormatsA, OpenMutexA, GetConsoleAliasesLengthA, CompareStringA, AreFileApisANSI, CreateFileW, EnumCalendarInfoExA, RequestWakeupLatency, GetConsoleAliasA, CreateFileA, SetComputerNameA, GetSystemWindowsDirectoryA, GetModuleHandleA, GlobalUnlock, FindFirstVolumeMountPointW, CreateDirectoryExW, GetLogicalDriveStringsA, ReadConsoleInputA, FindNextVolumeMountPointW, SearchPathW, MoveFileW, CallNamedPipeA, GetCurrentDirectoryW, GetDriveTypeW, CreateMailslotA, CommConfigDialogW, GetProcAddress, LocalAlloc, DeleteTimerQueueTimer, SetHandleInformation, CreateJobObjectW, WriteConsoleOutputAttribute, FindFirstVolumeA, InterlockedIncrement, LocalFlags, CloseHandle, GetTickCount, ZombifyActCtx, SetConsoleCtrlHandler, AddAtomA, GetThreadPriority, FreeEnvironmentStringsW, InterlockedExchange, GetConsoleTitleW, SetVolumeMountPointA, ClearCommError, lstrlenA, CreateDirectoryExA, LoadLibraryA, GlobalFindAtomA, TerminateJobObject, lstrcpynA, BackupSeek, GetSystemDirectoryA, VerSetConditionMask, EnumSystemLocalesW, InterlockedFlushSList, WritePrivateProfileSectionW, GetStringTypeExW, GetFileAttributesW, ActivateActCtx, ReadFile, ResetEvent, LocalShrink, LocalLock, GlobalCompact, SetCommState, WriteConsoleInputW, DeleteAtom, FindResourceW, GetConsoleSelectionInfo, CreateIoCompletionPort, GetPrivateProfileStructA, ConvertThreadToFiber, InterlockedExchangeAdd, EnumCalendarInfoW, GetConsoleMode, EnumCalendarInfoA, GetConsoleAliasExesLengthA, CopyFileA, InterlockedDecrement, HeapAlloc, GetLastError, DeleteFileA, GetStartupInfoW, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, HeapFree, VirtualFree, VirtualAlloc, HeapReAlloc, HeapCreate, GetModuleHandleW, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetCurrentThreadId, HeapSize, GetModuleFileNameW, GetEnvironmentStringsW, GetCommandLineW, SetHandleCount, GetFileType, GetStartupInfoA, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, RaiseException, InitializeCriticalSectionAndSpinCount, RtlUnwind, WideCharToMultiByte, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, GetConsoleCP, FlushFileBuffers, SetFilePointer, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, SetStdHandle

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
Raeto-Romance	Switzerland	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.362.204.41.794 9801802027700 12/13/22-20:09:37.904526	TCP	2027700	ET TROJAN Amadey CnC Check-In	49801	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9764802027700 12/13/22-20:09:24.415498	TCP	2027700	ET TROJAN Amadey CnC Check-In	49764	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9749802027700 12/13/22-20:09:18.397632	TCP	2027700	ET TROJAN Amadey CnC Check-In	49749	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9767802027700 12/13/22-20:09:25.222687	TCP	2027700	ET TROJAN Amadey CnC Check-In	49767	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9795802027700 12/13/22-20:09:35.735518	TCP	2027700	ET TROJAN Amadey CnC Check-In	49795	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9770802027700 12/13/22-20:09:26.190276	TCP	2027700	ET TROJAN Amadey CnC Check-In	49770	80	192.168.2.3	62.204.41.79
192.168.2.3185.246.221.1 5149699802851815 12/13/22-20:08:50.072694	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49699	80	192.168.2.3	185.246.221.151
192.168.2.362.204.41.794 9740802027700 12/13/22-20:09:15.487438	TCP	2027700	ET TROJAN Amadey CnC Check-In	49740	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9798802027700 12/13/22-20:09:36.748511	TCP	2027700	ET TROJAN Amadey CnC Check-In	49798	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9746802027700 12/13/22-20:09:17.426965	TCP	2027700	ET TROJAN Amadey CnC Check-In	49746	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9743802027700 12/13/22-20:09:16.449856	TCP	2027700	ET TROJAN Amadey CnC Check-In	49743	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9761802027700 12/13/22-20:09:23.806620	TCP	2027700	ET TROJAN Amadey CnC Check-In	49761	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9752802027700 12/13/22-20:09:21.874851	TCP	2027700	ET TROJAN Amadey CnC Check-In	49752	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9771802027700 12/13/22-20:09:26.565033	TCP	2027700	ET TROJAN Amadey CnC Check-In	49771	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9802802027700 12/13/22-20:09:39.191576	TCP	2027700	ET TROJAN Amadey CnC Check-In	49802	80	192.168.2.3	62.204.41.79

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.362.204.41.794 9748802027700 12/13/22-20:09:18.100262	TCP	2027700	ET TROJAN Amadey CnC Check-In	49748	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9777802027700 12/13/22-20:09:30.589327	TCP	2027700	ET TROJAN Amadey CnC Check-In	49777	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9742802027700 12/13/22-20:09:16.147180	TCP	2027700	ET TROJAN Amadey CnC Check-In	49742	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9794802027700 12/13/22-20:09:35.428306	TCP	2027700	ET TROJAN Amadey CnC Check-In	49794	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9789802027700 12/13/22-20:09:34.068418	TCP	2027700	ET TROJAN Amadey CnC Check-In	49789	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9754802027700 12/13/22-20:09:22.487126	TCP	2027700	ET TROJAN Amadey CnC Check-In	49754	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9782802027700 12/13/22-20:09:32.020133	TCP	2027700	ET TROJAN Amadey CnC Check-In	49782	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9747802027700 12/13/22-20:09:17.691856	TCP	2027700	ET TROJAN Amadey CnC Check-In	49747	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9760802027700 12/13/22-20:09:23.551005	TCP	2027700	ET TROJAN Amadey CnC Check-In	49760	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9776802027700 12/13/22-20:09:30.348436	TCP	2027700	ET TROJAN Amadey CnC Check-In	49776	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9753802027700 12/13/22-20:09:22.159892	TCP	2027700	ET TROJAN Amadey CnC Check-In	49753	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9759802027700 12/13/22-20:09:23.268020	TCP	2027700	ET TROJAN Amadey CnC Check-In	49759	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9783802027700 12/13/22-20:09:32.395745	TCP	2027700	ET TROJAN Amadey CnC Check-In	49783	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9807802027700 12/13/22-20:09:40.738951	TCP	2027700	ET TROJAN Amadey CnC Check-In	49807	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9788802027700 12/13/22-20:09:33.792525	TCP	2027700	ET TROJAN Amadey CnC Check-In	49788	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9765802027700 12/13/22-20:09:24.668106	TCP	2027700	ET TROJAN Amadey CnC Check-In	49765	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9787802027700 12/13/22-20:09:33.525784	TCP	2027700	ET TROJAN Amadey CnC Check-In	49787	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9790802027700 12/13/22-20:09:34.337562	TCP	2027700	ET TROJAN Amadey CnC Check-In	49790	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9796802027700 12/13/22-20:09:36.034730	TCP	2027700	ET TROJAN Amadey CnC Check-In	49796	80	192.168.2.3	62.204.41.79

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.362.204.41.794 9781802027700 12/13/22-20:09:31.753391	TCP	2027700	ET TROJAN Amadey CnC Check-In	49781	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9772802027700 12/13/22-20:09:29.469495	TCP	2027700	ET TROJAN Amadey CnC Check-In	49772	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9735802027700 12/13/22-20:09:14.280167	TCP	2027700	ET TROJAN Amadey CnC Check-In	49735	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9741802027700 12/13/22-20:09:15.797540	TCP	2027700	ET TROJAN Amadey CnC Check-In	49741	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9799802027700 12/13/22-20:09:37.255404	TCP	2027700	ET TROJAN Amadey CnC Check-In	49799	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9766802027700 12/13/22-20:09:24.922545	TCP	2027700	ET TROJAN Amadey CnC Check-In	49766	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9803802027700 12/13/22-20:09:39.585529	TCP	2027700	ET TROJAN Amadey CnC Check-In	49803	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9806802027700 12/13/22-20:09:40.381114	TCP	2027700	ET TROJAN Amadey CnC Check-In	49806	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9757802027700 12/13/22-20:09:23.006710	TCP	2027700	ET TROJAN Amadey CnC Check-In	49757	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9778802027700 12/13/22-20:09:30.907345	TCP	2027700	ET TROJAN Amadey CnC Check-In	49778	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9775802027700 12/13/22-20:09:30.081643	TCP	2027700	ET TROJAN Amadey CnC Check-In	49775	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9793802027700 12/13/22-20:09:35.174611	TCP	2027700	ET TROJAN Amadey CnC Check-In	49793	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9800802027700 12/13/22-20:09:37.581033	TCP	2027700	ET TROJAN Amadey CnC Check-In	49800	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9784802027700 12/13/22-20:09:32.706051	TCP	2027700	ET TROJAN Amadey CnC Check-In	49784	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9769802027700 12/13/22-20:09:25.868942	TCP	2027700	ET TROJAN Amadey CnC Check-In	49769	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9774802027700 12/13/22-20:09:29.736811	TCP	2027700	ET TROJAN Amadey CnC Check-In	49774	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9805802027700 12/13/22-20:09:40.125674	TCP	2027700	ET TROJAN Amadey CnC Check-In	49805	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9768802027700 12/13/22-20:09:25.563234	TCP	2027700	ET TROJAN Amadey CnC Check-In	49768	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9751802027700 12/13/22-20:09:20.733567	TCP	2027700	ET TROJAN Amadey CnC Check-In	49751	80	192.168.2.3	62.204.41.79

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.362.204.41.794 9786802027700 12/13/22-20:09:33.253065	TCP	2027700	ET TROJAN Amadey CnC Check-In	49786	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9791802027700 12/13/22-20:09:34.581849	TCP	2027700	ET TROJAN Amadey CnC Check-In	49791	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9739802027700 12/13/22-20:09:15.157831	TCP	2027700	ET TROJAN Amadey CnC Check-In	49739	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9745802027700 12/13/22-20:09:17.106517	TCP	2027700	ET TROJAN Amadey CnC Check-In	49745	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9750802027700 12/13/22-20:09:19.302564	TCP	2027700	ET TROJAN Amadey CnC Check-In	49750	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9792802027700 12/13/22-20:09:34.882839	TCP	2027700	ET TROJAN Amadey CnC Check-In	49792	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9779802027700 12/13/22-20:09:31.163445	TCP	2027700	ET TROJAN Amadey CnC Check-In	49779	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9785802027700 12/13/22-20:09:32.996655	TCP	2027700	ET TROJAN Amadey CnC Check-In	49785	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9744802027700 12/13/22-20:09:16.793275	TCP	2027700	ET TROJAN Amadey CnC Check-In	49744	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9780802027700 12/13/22-20:09:31.434688	TCP	2027700	ET TROJAN Amadey CnC Check-In	49780	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9738802027700 12/13/22-20:09:14.724261	TCP	2027700	ET TROJAN Amadey CnC Check-In	49738	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9762802027700 12/13/22-20:09:24.088211	TCP	2027700	ET TROJAN Amadey CnC Check-In	49762	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9804802027700 12/13/22-20:09:39.864342	TCP	2027700	ET TROJAN Amadey CnC Check-In	49804	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9756802027700 12/13/22-20:09:22.763314	TCP	2027700	ET TROJAN Amadey CnC Check-In	49756	80	192.168.2.3	62.204.41.79
192.168.2.362.204.41.794 9797802027700 12/13/22-20:09:36.311423	TCP	2027700	ET TROJAN Amadey CnC Check-In	49797	80	192.168.2.3	62.204.41.79

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 13, 2022 20:07:42.480623960 CET	49696	443	192.168.2.3	204.79.197.200
Dec 13, 2022 20:07:42.480819941 CET	49696	443	192.168.2.3	204.79.197.200
Dec 13, 2022 20:07:42.480911970 CET	49696	443	192.168.2.3	204.79.197.200
Dec 13, 2022 20:07:42.480976105 CET	49696	443	192.168.2.3	204.79.197.200
Dec 13, 2022 20:07:42.481025934 CET	49696	443	192.168.2.3	204.79.197.200
Dec 13, 2022 20:07:42.481070042 CET	49696	443	192.168.2.3	204.79.197.200
Dec 13, 2022 20:07:42.481070042 CET	49696	443	192.168.2.3	204.79.197.200
Dec 13, 2022 20:07:42.481122017 CET	49696	443	192.168.2.3	204.79.197.200
Dec 13, 2022 20:07:42.481122017 CET	49696	443	192.168.2.3	204.79.197.200
Dec 13, 2022 20:07:42.481149912 CET	49696	443	192.168.2.3	204.79.197.200

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 13, 2022 20:07:42.497251034 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497309923 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497323036 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497344017 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497356892 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497369051 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497384071 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497395992 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497407913 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497435093 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497454882 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497478008 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497489929 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497509003 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497519970 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497534037 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497550964 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497562885 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497575045 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497637987 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497654915 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497673035 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497709036 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497792006 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497962952 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.497994900 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498008966 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498027086 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498070955 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498157024 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498172045 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498234034 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498311043 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498339891 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498711109 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498748064 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498764038 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498778105 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498791933 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498806000 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498836040 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498893023 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498908043 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498922110 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.498943090 CET	49696	443	192.168.2.3	204.79.197.200
Dec 13, 2022 20:07:42.499001026 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499070883 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499119997 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499161959 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499176979 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499238968 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499279022 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499293089 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499314070 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499327898 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499346972 CET	49696	443	192.168.2.3	204.79.197.200
Dec 13, 2022 20:07:42.499414921 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499428034 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499474049 CET	443	49696	204.79.197.200	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 13, 2022 20:07:42.499511957 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499553919 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499651909 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499667883 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499681950 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499711037 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499795914 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499833107 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499859095 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499872923 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.499912977 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.500003099 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.500039101 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.500052929 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.547748089 CET	443	49696	204.79.197.200	192.168.2.3
Dec 13, 2022 20:07:42.547856092 CET	49696	443	192.168.2.3	204.79.197.200
Dec 13, 2022 20:07:49.880563021 CET	49697	443	192.168.2.3	23.35.236.109
Dec 13, 2022 20:07:49.880621910 CET	443	49697	23.35.236.109	192.168.2.3
Dec 13, 2022 20:07:49.880705118 CET	49697	443	192.168.2.3	23.35.236.109
Dec 13, 2022 20:07:49.881911993 CET	49697	443	192.168.2.3	23.35.236.109
Dec 13, 2022 20:07:49.881938934 CET	443	49697	23.35.236.109	192.168.2.3
Dec 13, 2022 20:07:49.967329025 CET	443	49697	23.35.236.109	192.168.2.3
Dec 13, 2022 20:07:49.967442036 CET	49697	443	192.168.2.3	23.35.236.109
Dec 13, 2022 20:07:49.976569891 CET	49697	443	192.168.2.3	23.35.236.109
Dec 13, 2022 20:07:49.976596117 CET	443	49697	23.35.236.109	192.168.2.3
Dec 13, 2022 20:07:49.977266073 CET	443	49697	23.35.236.109	192.168.2.3
Dec 13, 2022 20:07:50.008229017 CET	49697	443	192.168.2.3	23.35.236.109
Dec 13, 2022 20:07:50.008261919 CET	443	49697	23.35.236.109	192.168.2.3
Dec 13, 2022 20:07:50.027926922 CET	443	49697	23.35.236.109	192.168.2.3
Dec 13, 2022 20:07:50.028023958 CET	443	49697	23.35.236.109	192.168.2.3
Dec 13, 2022 20:07:50.028126955 CET	49697	443	192.168.2.3	23.35.236.109

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 13, 2022 20:08:50.016643047 CET	192.168.2.3	8.8.8.8	0xa2e4	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:50.661819935 CET	192.168.2.3	8.8.8.8	0x6732	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:51.177598953 CET	192.168.2.3	8.8.8.8	0x5841	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:51.364558935 CET	192.168.2.3	8.8.8.8	0xdcbf	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:51.559534073 CET	192.168.2.3	8.8.8.8	0x18e8	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:51.750485897 CET	192.168.2.3	8.8.8.8	0xe2e0	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:52.020116091 CET	192.168.2.3	8.8.8.8	0x3671	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:52.202105045 CET	192.168.2.3	8.8.8.8	0xd855	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:52.385538101 CET	192.168.2.3	8.8.8.8	0x7d94	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:52.649854898 CET	192.168.2.3	8.8.8.8	0xc32b	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:52.840059996 CET	192.168.2.3	8.8.8.8	0xae2a	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:53.015722990 CET	192.168.2.3	8.8.8.8	0x149c	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:53.208112001 CET	192.168.2.3	8.8.8.8	0xdba4	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:53.383039951 CET	192.168.2.3	8.8.8.8	0xeed4	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 13, 2022 20:08:53.555284977 CET	192.168.2.3	8.8.8.8	0x39fa	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:53.723181963 CET	192.168.2.3	8.8.8.8	0xc81d	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:53.919317007 CET	192.168.2.3	8.8.8.8	0x1a49	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:54.089325905 CET	192.168.2.3	8.8.8.8	0xa128	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:54.255630016 CET	192.168.2.3	8.8.8.8	0xda09	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:54.435497046 CET	192.168.2.3	8.8.8.8	0x4194	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:54.606698036 CET	192.168.2.3	8.8.8.8	0xef8d	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:54.785937071 CET	192.168.2.3	8.8.8.8	0xd15d	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:54.950651884 CET	192.168.2.3	8.8.8.8	0x1964	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:55.123325109 CET	192.168.2.3	8.8.8.8	0x4828	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:55.290416002 CET	192.168.2.3	8.8.8.8	0x3cfd	Standard query (0)	kikangalaassociates.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:56.201690912 CET	192.168.2.3	8.8.8.8	0x915d	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:56.441494942 CET	192.168.2.3	8.8.8.8	0xc783	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:58.035155058 CET	192.168.2.3	8.8.8.8	0x9924	Standard query (0)	r3oidsofsios.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 13, 2022 20:08:50.035814047 CET	8.8.8.8	192.168.2.3	0xa2e4	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:51.017219067 CET	8.8.8.8	192.168.2.3	0x6732	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:51.205988884 CET	8.8.8.8	192.168.2.3	0x5841	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:51.385179043 CET	8.8.8.8	192.168.2.3	0xdcbf	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:51.578742981 CET	8.8.8.8	192.168.2.3	0x18e8	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:51.856148958 CET	8.8.8.8	192.168.2.3	0xe2e0	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:52.037960052 CET	8.8.8.8	192.168.2.3	0x3671	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:52.219321012 CET	8.8.8.8	192.168.2.3	0xd855	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:52.493618965 CET	8.8.8.8	192.168.2.3	0x7d94	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:52.667063951 CET	8.8.8.8	192.168.2.3	0xc32b	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:52.859112024 CET	8.8.8.8	192.168.2.3	0xae2a	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:53.034872055 CET	8.8.8.8	192.168.2.3	0x149c	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:53.225176096 CET	8.8.8.8	192.168.2.3	0xdba4	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 13, 2022 20:08:53.402158022 CET	8.8.8.8	192.168.2.3	0xeed4	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:53.573211908 CET	8.8.8.8	192.168.2.3	0x39fa	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:53.742464066 CET	8.8.8.8	192.168.2.3	0xc81d	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:53.936579943 CET	8.8.8.8	192.168.2.3	0x1a49	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:54.106309891 CET	8.8.8.8	192.168.2.3	0xa128	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:54.274415970 CET	8.8.8.8	192.168.2.3	0xda09	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:54.454756975 CET	8.8.8.8	192.168.2.3	0x4194	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:54.623677015 CET	8.8.8.8	192.168.2.3	0xef8d	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:54.803195000 CET	8.8.8.8	192.168.2.3	0xd15d	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:54.967981100 CET	8.8.8.8	192.168.2.3	0x1964	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:55.140712023 CET	8.8.8.8	192.168.2.3	0x4828	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:55.325320959 CET	8.8.8.8	192.168.2.3	0x3cfd	No error (0)	kikangalaassociates.com		185.98.131.207	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:56.218902111 CET	8.8.8.8	192.168.2.3	0x915d	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:56.458796024 CET	8.8.8.8	192.168.2.3	0xc783	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false
Dec 13, 2022 20:08:58.052490950 CET	8.8.8.8	192.168.2.3	0x9924	No error (0)	r3oidsofsios.com		185.246.221.151	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

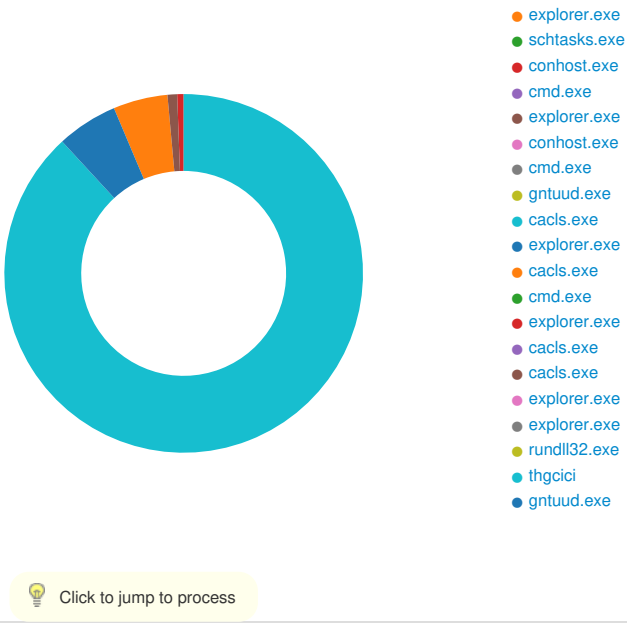
- fs.microsoft.com
- kikangalaassociates.com
- login.live.com
- iglyuyotce.org
  - r3oidsofsios.com
- csigrnv.com
- sigiagum.org
- rdpcbv.net
- arfujedsl.net
- nvtalqe.net
- bprujbtf.com

- ecaapsyol.com
- xmhgchsawe.net
- qmwhbha.net
- hhqusu.net
- nvtkvayro.org
- aroxyrayv.com
- ufutmn.net
- gomlgu.com
- mqmkmifvh.org
- okpnuoeb.net
- prhgrykwf.org
- umgkkbyv.org
- bljwplujsw.com
- jqdieq.net
- qrlpwddo.net
- hmsoq.net
- rwsblto.com
- ikihxohlb.com
- sdeypctxsi.net
- 31.41.244.228
- jenhfc.net
- 62.204.41.79

Statistics

Behavior

- kmxId0uLRn.exe
- explorer.exe
- thgcici
- 8F68.exe
- conhost.exe
- 9545.exe
- explorer.exe
- explorer.exe
- explorer.exe
- WerFault.exe
- gntuud.exe



System Behavior

Analysis Process: kmxId0uLRn.exe PID: **5936**, Parent PID: **3452**

General	
Target ID:	0
Start time:	20:07:45
Start date:	13/12/2022
Path:	C:\Users\user\Desktop\kmxId0uLRn.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\kmxId0uLRn.exe
Imagebase:	0x400000
File size:	244736 bytes
MD5 hash:	C8782DA2928F63712D03D0EA36C57C3F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000003.263185446.00000000005E0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.354414685.0000000000601000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.354414685.0000000000601000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.354377233.00000000005E0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.354377233.00000000005E0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.354530381.0000000000631000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.354314042.00000000005D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3452**, Parent PID: **5936**

General	
Target ID:	1
Start time:	20:07:57
Start date:	13/12/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE

Imagebase:	0x7ff69fe90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000000.344354545.0000000005791000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000000.344354545.0000000005791000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

Analysis Process: thgcici PID: **2108**, Parent PID: **1080**

General

Target ID:	11
Start time:	20:08:51
Start date:	13/12/2022
Path:	C:\Users\user\AppData\Roaming\thgcici
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\thgcici
Imagebase:	0x400000
File size:	244736 bytes
MD5 hash:	C8782DA2928F63712D03D0EA36C57C3F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.458517384.00000000020F1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000B.00000002.458517384.00000000020F1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000B.00000002.456935359.00000000006C1000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000B.00000002.456463598.00000000006A0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.458480142.00000000020D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000B.00000002.458480142.00000000020D0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000003.425062940.0000000002090000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 69%, ReversingLabs
Reputation:	low

Analysis Process: 8F68.exe PID: **1568**, Parent PID: **3452**

General

Target ID:	12
Start time:	20:08:55
Start date:	13/12/2022
Path:	C:\Users\user\AppData\Local\Temp\8F68.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8F68.exe
Imagebase:	0xc10000
File size:	559616 bytes
MD5 hash:	46F30465FA693033E7D3D78468406C0C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000C.00000000.404562471.0000000000C42000.00000004.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000C.00000000.416200644.0000000000C42000.00000004.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000C.00000002.443923174.0000000000C42000.00000004.00000001.01000000.00000009.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	0d		success or wait	1	C270D7	WriteFile
\Device\ConDrv	3	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	C270D7	WriteFile

Analysis Process: conhost.exe PID: **1324**, Parent PID: **1568**

General

Target ID:	13
Start time:	20:08:55
Start date:	13/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 9545.exe PID: **6140**, Parent PID: **3452**

General

Target ID:	14
Start time:	20:08:56
Start date:	13/12/2022
Path:	C:\Users\user\AppData\Local\Temp\9545.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\9545.exe
Imagebase:	0xdd0000
File size:	249344 bytes
MD5 hash:	C6524CC2CB091E23BE6D9526D6BCBC99
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000000E.00000000.403627141.0000000000DD1000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000000E.00000000.403992347.0000000000DD1000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000000E.00000000.402947790.0000000000DD1000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000000E.00000002.418854109.0000000000DD1000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000000E.00000000.403831524.0000000000DD1000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Temp\9545.exe, Author: Joe Security

Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 53%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2c33368f7d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	DDB783	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	DDB8CF	CopyFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 58 48 fd fd 36 1b fd fd 36 1b fd fd 36 1b fd fd 35 1a fd fd 36 1b fd fd 33 1a 61 fd 36 1b fd fd 32 1a fd fd 36 1b 28 fd 32 1a fd fd 36 1b 28 fd 35 1a fd fd 36 1b 28 fd 33 1a fd fd 36 1b fd fd 37 1a fd fd 36 1b fd fd 37 1b 5c fd 36 1b 66 fd 3f 1a fd fd 36 1b 66 fd fd 1b fd fd 36 1b 66 fd 34 1a fd fd 36 1b 52 69 63 68 fd fd 36 1b 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ@!L!This program cannot be run in DOS mode.$XH666563a626(26(56(36767\6f?6f6f46Rich6PEL	success or wait	2	DDB8CF	CopyFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: **2096**, Parent PID: **3452**

General

Target ID:	17
Start time:	20:08:57
Start date:	13/12/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xe20000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000011.00000000.405174014.00000000004F0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

Analysis Process: explorer.exe PID: **3940**, Parent PID: **3452**

General

Target ID:	18
Start time:	20:09:00
Start date:	13/12/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe
Imagebase:	0x7ff69fe90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: **1020**, Parent PID: **3452**

General

Target ID:	19
Start time:	20:09:03
Start date:	13/12/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xe20000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader, Description: Yara detected SmokeLoader, Source: 00000013.00000002.775997702.0000000000521000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000013.00000000.417309353.0000000000530000.00000040.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

Analysis Process: WerFault.exe PID: **2292**, Parent PID: **1568**

General

Target ID:	20
Start time:	20:09:03
Start date:	13/12/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1568 -s 268
Imagebase:	0xfa0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language

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	6FAF1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER92B2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER92B2.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_8F68.exe_a1299b47a4636d69dc3bf7715d1130fd3baa11_d5638d9e_08cf2d1b	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_8F68.exe_a1299b47a4636d69dc3bf7715d1130fd3baa11_d5638d9e_08cf2d1b\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FAE497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER92B2.tmp	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER92B2.tmp.xml	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER92FE.tmp.csv	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94F3.tmp.txt	success or wait	1	6FAE497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 60 4c fd 63 fd 05 12 00 00 00 00 00	MDMP `Lc	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	3892	6	00 00 00 00 00 00		success or wait	1	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 34 0f 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 20 06 00 00 57 4c fd 63 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 20 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UB4GenuineIntelWTWLc Pacific Standard TimePacific Daylight Time	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	4230	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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd 00 00 00 00 00 37 fd 1c 01 60 01 00 00 00 00 00 00 fd 7f fd 00 fd fd 35 01 fd 7f fd 00 23 00 00 00 06 02 01 00 fd fd 35 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++7`5#5+	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	1620	168	6c 05 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 7f fd 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 10 00 00	l	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	7094	20	12 00 00 00 7b 7f fd 00 00 00 00 00 00 01 00 00 fd 1c 00 00	{	success or wait	18	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	7386	256	08 72 06 fd fd fd fd 00 00 66 3b 75 08 72 05 05 fd fd 00 00 66 3b fd 75 0e 66 fd fd 74 05 fd fd 02 fd fd 33 fd fd 03 33 fd 40 5f 5e 5b 5d fd 08 00 55 fd fd 64 fd 30 00 00 00 56 57 fd 40 0c fd 78 0c fd fd 75 08 fd 76 30 fd 74 fd fd fd fd fd 74 0a fd 36 3b fd 75 fd 33 fd fd 03 fd 46 18 5f 5e 5d fd 04 00 55 fd fd fd 24 04 00 00 fd 7d 08 00 53 56 57 0f fd fd 05 00 00 fd 7d 10 00 0f fd fd 05 00 00 6a 6b 58 6a 65 59 6a 72 66 fd 45 fd 58 6a 6e 5e 6a 6c 5f 6a 33 66 fd 45 fd 58 6a 32 66 fd 45 fd 58 6a 2e 5a 6a 64 66 fd 45 fd 33 fd 66 fd 4d fd 66 fd 4d fd 59 66 fd 45 fd 6a 74 58 66 fd 45 fd 33 fd 66 fd 45 fd fd 45 fd 50 66 fd 75 fd 66 fd 7d fd 66 fd 55 fd 66 fd 4d fd 66 fd 7d fd 66 fd 7d fd 66 fd 75 fd 66 fd 4d fd 66 fd 7d fd 66 fd 7d fd 66 fd 55 fd 66 fd 4d	rf;urf;uft33@_^[]Ud0VW@xuv0tt6;u3F_^]U$}SVW}jkXjeYjrfEXjn^jl_j3fEXj2fEXj.ZjdfE3fMfMYfEjtXfE3fEEPfuf}fUfMf}f}fufMf}f}fUfM	success or wait	17	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	26442	4096	fd fd fd 01 00 00 fd 01 00 fd fd 01 00 00 00 00 00 1e 00 00 00 00 00 00 00 30 1d 01 00 00 00 00 20 06 00 00 74 11 00 00 00 00 00 00 00 00 00 00 00 fd 1c 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 7f 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0 tpw	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	4946	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd 35 01 fd fd fd 77 23 00 00 00 02 02 00 00 38 fd 35 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++5w#85+	success or wait	3	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	1888	48	74 11 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 30 1d 01 00 00 00 00 fd fd fd 01 00 00 00 00 18 04 00 00 fd 26 00 00 fd 02 00 00 fd 18 00 00	t 0&	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	1948	4	0c 00 00 00		success or wait	12	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	3898	22	10 00 00 00 38 00 46 00 36 00 38 00 2e 00 65 00 78 00 65 00 00 00	8F68.exe	success or wait	12	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	3140	752	00 00 fd 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 6e 10 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 50 fd 02 00 00 00 00 00 70 fd 02 00 00 00 00 fd 39 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 7f 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 1d 2a 1b 00 00 00 00 00 23 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 65 08 05 00 00 00 00	t`A!-anBB? #@AZbPp9*#@e	success or wait	1	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	30538	4356	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8CD4.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 14 05 00 00 fd 07 00 00 05 00 00 00 24 01 00 00 fd 1b 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 0a 00 00 76 7d 00 00 15 00 00 00 fd 01 00 00 fd 0c 00 00 16 00 00 00 fd 00 00 00 fd 0e 00 00	$T8Tv}	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 35 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1568</Pid>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 38 00 46 00 36 00 38 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>8F68.exe</ImageName>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1072	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 32 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000002</CmdLineSignature>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1170	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 38 00 39 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>9898</Uptime>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1212	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1216	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1220	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1302	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1306	2	09 00		success or wait	2	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1310	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1362	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1366	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1370	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1414	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1418	2	09 00		success or wait	3	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1424	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 35 00 39 00 39 00 33 00 39 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>45993984</PeakVirtualSize>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1510	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1514	2	09 00		success or wait	3	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1520	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 35 00 39 00 38 00 35 00 37 00 39 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>45985792</VirtualSize>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1590	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1594	2	09 00		success or wait	3	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1600	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 33 00 30 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	<PageFaultCount>1301</PageFaultCount>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1674	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1678	2	09 00		success or wait	3	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1684	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 34 00 37 00 31 00 38 00 35 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>4718592</PeakWorkingSetSize>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1780	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1784	2	09 00		success or wait	3	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1790	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 34 00 37 00 31 00 38 00 35 00 39 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>4718592</WorkingSetSize>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1870	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1874	2	09 00		success or wait	3	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1880	112	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 38 00 36 00 36 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>86600</QuotaPeakPagedPoolUsage>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1992	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	1996	2	09 00		success or wait	3	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2002	96	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 38 00 36 00 35 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>86560</QuotaPagedPoolUsage>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2098	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2102	2	09 00		success or wait	3	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2108	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 30 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>15016</QuotaPeakNonPagedPoolUsage>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2232	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2236	2	09 00		success or wait	3	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2242	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>14664</QuotaNonPagedPoolUsage>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2350	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2354	2	09 00		success or wait	3	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2360	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 38 00 32 00 30 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1282048</PagefileUsage>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2436	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2440	2	09 00		success or wait	3	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2446	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 39 00 34 00 33 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1294336</PeakPagefileUsage>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2538	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2542	2	09 00		success or wait	3	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2548	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 38 00 32 00 30 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1282048</PrivateUsage>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2620	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2624	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2628	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2674	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2678	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2682	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	3	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2722	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2762	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2766	2	09 00		success or wait	4	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2774	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2804	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2808	2	09 00		success or wait	4	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2816	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2886	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2890	2	09 00		success or wait	4	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2898	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2988	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	2992	2	09 00		success or wait	4	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3000	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 38 00 33 00 37 00 32 00 37 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>3837270</Uptime>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3060	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3138	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3142	2	09 00		success or wait	4	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3150	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3202	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3206	2	09 00		success or wait	4	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3214	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3258	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3262	2	09 00		success or wait	5	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3272	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3376	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3450	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3454	2	09 00		success or wait	5	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3464	78	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 35 00 35 00 37 00 34 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>155746</PageFaultCount>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3542	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3546	2	09 00		success or wait	5	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3556	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 35 00 32 00 36 00 37 00 34 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	<PeakWorkingSetSize>152674304</PeakWorkingSetSize>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3656	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3660	2	09 00		success or wait	5	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3670	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 35 00 31 00 39 00 32 00 30 00 36 00 34 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>151920640</WorkingSetSize>	success or wait	1	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3754	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3758	2	09 00		success or wait	5	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3768	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 34 00 32 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11429 52</QuotaPeakPagedPoolUsage>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3884	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3888	2	09 00		success or wait	5	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3898	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 39 00 31 00 39 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1091920</ QuotaPagedPoolUsage>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	3998	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4002	2	09 00		success or wait	5	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4012	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 33 00 35 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>14 3528</QuotaPeakNonPagedPoolUsage>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4138	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4142	2	09 00		success or wait	5	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4152	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 35 00 39 00 36 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	<QuotaNonPagedPoolUsage>85968< /QuotaNonPagedPoolUsage>	success or wait	1	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4260	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4264	2	09 00		success or wait	5	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4274	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 34 00 32 00 32 00 39 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>48422912</PagefileUsage>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4352	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4356	2	09 00		success or wait	5	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4366	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 39 00 39 00 32 00 32 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>48992256</PeakPagefileUsage>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4460	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4464	2	09 00		success or wait	5	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4474	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 34 00 32 00 32 00 39 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>48422912</PrivateUsage>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4548	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4552	2	09 00		success or wait	4	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4560	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4606	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4610	2	09 00		success or wait	3	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4616	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	2	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4666	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4698	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4702	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4704	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4752	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4790	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4794	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4798	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4850	4	0d 00 0a 00		success or wait	9	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4854	2	09 00		success or wait	18	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	4858	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 38 00 46 00 36 00 38 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>8F68.exe</Parameter0>	success or wait	9	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	5512	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	5516	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	5518	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	5558	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	5562	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	5564	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	5602	4	0d 00 0a 00		success or wait	6	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	5606	2	09 00		success or wait	12	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	5610	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6164	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6168	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6170	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6210	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6214	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6216	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6254	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6258	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6262	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6356	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6360	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6364	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 6f 00 6a 00 75 00 68 00 65 00 77 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>ojuhew, Inc.</SystemManufacturer>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6470	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6474	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6478	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 6f 00 6a 00 75 00 68 00 65 00 77 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>ojuhew7,1</SystemProductName>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6574	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6578	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6582	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6702	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6706	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6710	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 32 00 37 00 37 00 39 00 39 00 33 00 37 00 38 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1627799378</OSInstallDate>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6792	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6796	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6800	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6902	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6906	2	09 00		success or wait	2	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6910	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6978	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6982	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	6984	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7024	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7028	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7030	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7064	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7068	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7072	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7168	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7172	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7174	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7210	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7214	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7216	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7240	4	0d 00 0a 00		success or wait	3	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7244	2	09 00		success or wait	6	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7248	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 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7506	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7510	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7512	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7538	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7542	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7544	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 32 00 2d 00 31 00 32 00 2d 00 31 00 34 00 54 00 30 00 34 00 3a 00 30 00 39 00 3a 00 30 00 35 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-12-14T04:09:05Z">	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7644	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7648	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7652	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 32 00 39 00 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 35 00 36 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 39 00 38 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 39 00 38 00 34 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="293" PID="1568" UptimeMS="1984" TimeSinceCreationMS="1984" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7914	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7918	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7922	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7942	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7946	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7948	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7986	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7990	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	7992	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	8030	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	8034	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	8038	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 33 00 30 00 38 00 39 00 65 00 34 00 36 00 2d 00 62 00 31 00 36 00 30 00 2d 00 34 00 31 00 61 00 36 00 2d 00 39 00 38 00 33 00 34 00 2d 00 62 00 35 00 32 00 32 00 31 00 63 00 65 00 64 00 65 00 36 00 61 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>83089e46-b160-41a6-9834-b5221cede6a3</Guid>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	8136	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	8140	2	09 00		success or wait	2	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	8144	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 32 00 2d 00 31 00 32 00 2d 00 31 00 34 00 54 00 30 00 34 00 3a 00 30 00 39 00 3a 00 30 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	<CreationTime>2022-12-14T04:09:05Z</CreationTime>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	8242	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	8246	2	09 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	8248	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	8288	4	0d 00 0a 00		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER908E.tmp.WERInternalMetadata.xml	8292	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6FAE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER92B2.tmp.xml	0	4622	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_8F68.exe_a1299b47a4636d69dc3bf7715d1130fd3baa11_d5638d9e_08cf2d1b\Report.wer	0	2	fd fd		success or wait	1	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_8F68.exe_a1299b47a4636d69dc3bf7715d1130fd3baa11_d5638d9e_08cf2d1b\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	139	6FAE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_8F68.exe_a1299b47a4636d69dc3bf7715d1130fd3baa11_d5638d9e_08cf2d1b\Report.wer	8062	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 36 00 31 00 38 00 34 00 35 00 38 00 32 00 30 00 34 00	MetadataHash=-618458204	success or wait	1	6FAE497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: gntuud.exe PID: **5972**, Parent PID: **6140**

General

Target ID:	21
Start time:	20:09:04
Start date:	13/12/2022
Path:	C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe"
Imagebase:	0xf00000
File size:	249344 bytes
MD5 hash:	C6524CC2CB091E23BE6D9526D6BCBC99
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000015.00000003.498981390.0000000000C04000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000015.00000003.499037932.0000000000C14000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000015.00000000.417948151.0000000000F01000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000015.00000003.499443031.0000000000BC7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000015.00000003.499443031.0000000000BC7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000015.00000002.783235470.0000000000BB4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000015.00000002.783235470.0000000000BB4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 00000015.00000002.785970616.0000000000C07000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000015.00000002.788503094.0000000000F01000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 53%, ReversingLabs

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bf045808586a24	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F11CEC	CreateDirectoryA
C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	F08CE2	CreateFileA
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	F09EB0	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F09EB0	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F09EB0	HttpSendRequestA
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	F09EB0	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F09EB0	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F09EB0	HttpSendRequestA
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	F09EB0	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F09EB0	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F09EB0	HttpSendRequestA
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	F09EB0	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F09EB0	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F09EB0	HttpSendRequestA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\853321935212	success or wait	12	F1FDE3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll	0	16384	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	8	F08D47	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	16384	16384	fd fd fd fd fd cb 03 fd fd 74 10 fd fd fd 48 fd 39 fd 7c 02 fd fd fd 5b fd fd fd fd fd fd fd fd fd 3b 5f 5e 5b cb fd 53 56 51 fd fd 0b fd 33 4b fd fd 0a 00 00 00 fd 04 24 fd 04 24 5a 5e 5b fd 53 fd c9 fd 31 45 fd 74 05 fd 4b fd 29 fd 51 fd 16 fd fd fd 59 fd fd 5b fd fd fd fd f0 01 fd 5d fd fd fd c5 fd 74 10 50 6a 00 fd 04 fd fd fd fd fd 0f fd fd fd fd cd 40 00 fd 10 fd fd 74 06 52 fd fd fd fd fd cd 40 00 fd 10 fd fd 74 0e fd 00 00 00 00 00 50 52 fd fd fd fd 58 cd 40 00 53 56 fd c9 8b 03 fd fd 74 0c fd 03 00 00 00 00 50 fd fd fd fd fd fd 04 4e 75 fd 5e 5b cd 40 00 fd fd 0f fd fd fd fd fd 4a fd fd fd 0f fd fd fd fd fd 51 52 50 fd fd fd fd fd 0f fd 71 fd fd fd fd 53 56 57 55 fd fd 04	tH9| [;_^[SVQ3$$Z^[S1tK)QY[ ]tPj @tR@tPRX@SVtPNu^[@JQRPqSVWU	success or wait	5	F08D56	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\853321935212	unknown	4	success or wait	99247	F09877	ReadFile

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Startup	expand unicode	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	C:\Users\user\AppData\Local\Temp\2c33368f7d\	success or wait	1	F030C7	RegSetValueExA

Analysis Process: explorer.exe PID: **4044**, Parent PID: **3452**

General

Target ID:	22
Start time:	20:09:04
Start date:	13/12/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe
Imagebase:	0x7ff69fe90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader, Description: Yara detected SmokeLoader, Source: 00000016.00000002.774640150.00000000006B1000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: schtasks.exe PID: **1012**, Parent PID: **5972**

General

Target ID:	23
Start time:	20:09:06
Start date:	13/12/2022

Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN gntuud.exe /TR "C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe" /F
Imagebase:	0xd10000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 4944, Parent PID: 1012

General

Target ID:	24
Start time:	20:09:06
Start date:	13/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 504, Parent PID: 5972

General

Target ID:	25
Start time:	20:09:06
Start date:	13/12/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /k echo Y|CACLS "gntuud.exe" /P "user:N"&&CACLS "gntuud.exe" /P "user:R" /E&&echo Y|CACLS "..\2c33368f7d" /P "user:N"&&CACLS "..\2c33368f7d" /P "user:R" /E&&Exit
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: 4696, Parent PID: 3452

General

Target ID:	26
Start time:	20:09:06
Start date:	13/12/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xe20000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000001A.00000000.423609338.0000000000970000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Analysis Process: conhost.exe PID: **2300**, Parent PID: **504**

General	
Target ID:	27
Start time:	20:09:06
Start date:	13/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **4644**, Parent PID: **504**

General	
Target ID:	28
Start time:	20:09:07
Start date:	13/12/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" echo Y"
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: gntuud.exe PID: **3124**, Parent PID: **1080**

General	
Target ID:	29
Start time:	20:09:07
Start date:	13/12/2022
Path:	C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe

Imagebase:	0xf00000
File size:	249344 bytes
MD5 hash:	C6524CC2CB091E23BE6D9526D6BCBC99
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000001D.00000000.425029230.0000000000F01000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000001D.00000002.428729367.0000000000F01000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security

Analysis Process: cacls.exe PID: **3516**, Parent PID: **504**

General

Target ID:	30
Start time:	20:09:07
Start date:	13/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "gntuud.exe" /P "user:N"
Imagebase:	0x9e0000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **5536**, Parent PID: **3452**

General

Target ID:	31
Start time:	20:09:07
Start date:	13/12/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xe20000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000001F.00000000.426593885.0000000003450000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Analysis Process: cacls.exe PID: **5652**, Parent PID: **504**

General

Target ID:	32
Start time:	20:09:08
Start date:	13/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "gntuud.exe" /P "user:R" /E
Imagebase:	0x9e0000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5680**, Parent PID: **504**

General	
Target ID:	33
Start time:	20:09:09
Start date:	13/12/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" echo Y"
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **5692**, Parent PID: **3452**

General	
Target ID:	34
Start time:	20:09:09
Start date:	13/12/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xe20000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000022.00000000.429438818.00000000005F0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Analysis Process: cacls.exe PID: **5720**, Parent PID: **504**

General	
Target ID:	35
Start time:	20:09:09
Start date:	13/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "..\2c33368f7d" /P "user:N"
Imagebase:	0x9e0000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cacls.exe PID: **5868**, Parent PID: **504**

General	
Target ID:	36
Start time:	20:09:10
Start date:	13/12/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "..\2c33368f7d" /P "user:R" /E
Imagebase:	0x9e0000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **5896**, Parent PID: **3452**

General	
Target ID:	38
Start time:	20:09:10
Start date:	13/12/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe
Imagebase:	0x7ff69fe90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **1004**, Parent PID: **3452**

General	
Target ID:	40
Start time:	20:09:12
Start date:	13/12/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xe20000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000028.00000000.435504290.0000000000530000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Analysis Process: rundll32.exe PID: **4876**, Parent PID: **5972**

General	
Target ID:	41
Start time:	20:09:14
Start date:	13/12/2022

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\bf045808586a24\cred64.dll, Main
Imagebase:	0x2a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi

Analysis Process: thgcici PID: **4892**, Parent PID: **1080**

General

Target ID:	43
Start time:	20:10:01
Start date:	13/12/2022
Path:	C:\Users\user\AppData\Roaming\thgcici
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\thgcici
Imagebase:	0x400000
File size:	244736 bytes
MD5 hash:	C8782DA2928F63712D03D0EA36C57C3F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000002B.00000003.588957160.0000000000490000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000002B.00000002.605352083.0000000002101000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000002B.00000002.605352083.0000000002101000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000002B.00000002.603086862.0000000000490000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000002B.00000002.603086862.0000000000490000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000002B.00000002.603006628.0000000000470000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000002B.00000002.603522638.00000000004A4000.00000040.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: gntuud.exe PID: **3920**, Parent PID: **1080**

General

Target ID:	44
Start time:	20:10:01
Start date:	13/12/2022
Path:	C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2c33368f7d\gntuud.exe
Imagebase:	0xf00000
File size:	249344 bytes
MD5 hash:	C6524CC2CB091E23BE6D9526D6BCBC99
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000002C.00000000.541818627.000000000F01000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000002C.00000002.547069275.000000000F01000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security

Disassembly

No disassembly