ID: 682606
Sample Name:
valliant.document.08.11.2022.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:57:37
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

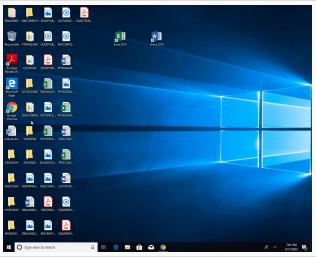
Windows Analysis Report

valliant.document.08.11.2022.doc

Overview

General Information

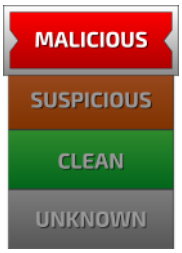
Sample Name:	valliant.document.08.11.2022.doc
Analysis ID:	682606
MD5:	cadb9d5ed47b8d..
SHA1:	f7197fa991510f9..
SHA256:	9cb01729327bd9..
Tags:	doc IcedID
Infos:	



Errors

⚠ Corrupt sample or wrongly selected analyzer.

Detection

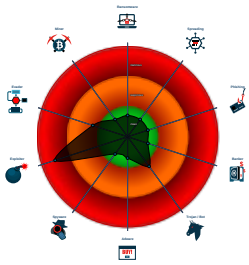


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 2908 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - WerFault.exe (PID: 1928 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2908 -s 4128 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 2072 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2908 -s 4132 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

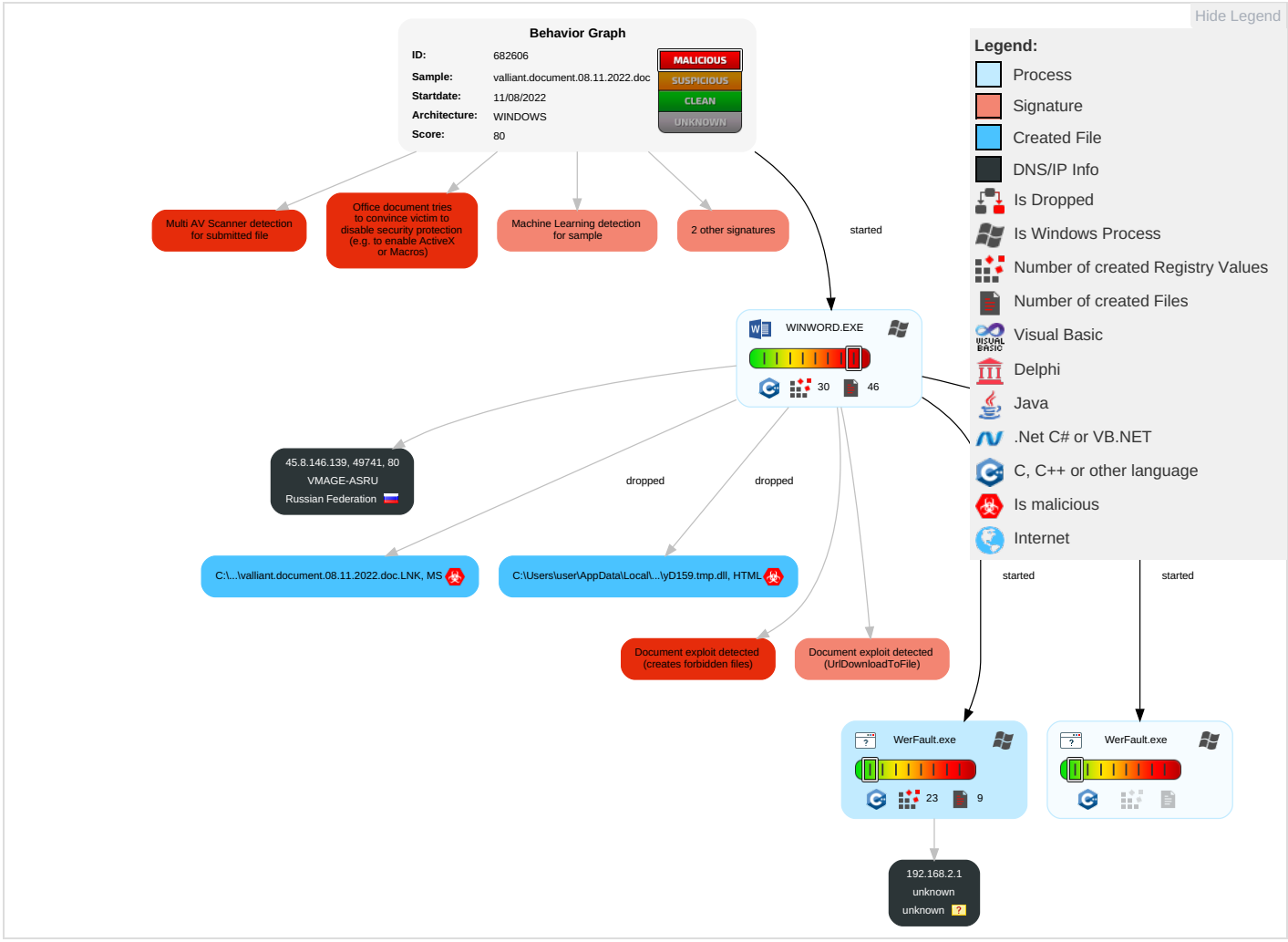
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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

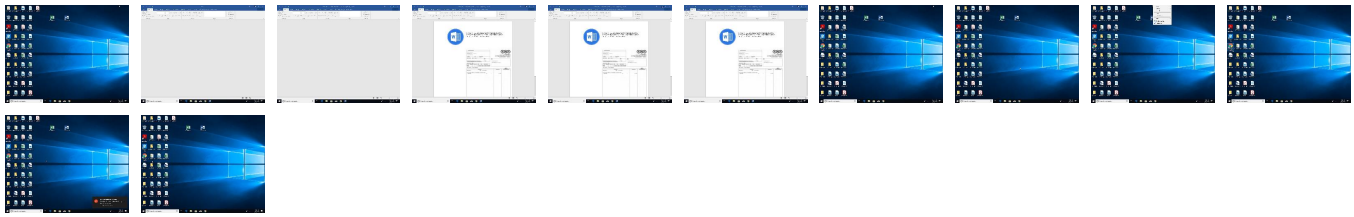
Behavior Graph



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
valliant.document.08.11.2022.doc	27%	Virustotal		Browse
valliant.document.08.11.2022.doc	18%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
valliant.document.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://cdn.entity.	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://settings.outlook.comS	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/SKWR8YXON-RX9R4781JWMO3UUH0NGDBO/-f71USERNAME=userUSERPROFILE=C:	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/Ep	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://https://my.microsoftpersonalcontent.com	0%	URL Reputation	safe	
http://45.8.146.139/fhfty/SKWR8YXON-RX9R4781JWMO3UUH0NGDBO/-fOOC:	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://substrate.office.comp	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/ym	0%	Avira URL Cloud	safe	
http://45.8.146.139/fhfty/SKWR8YXON-RX9R4781JWMO3UUH0NGDBO/-f	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com2p7	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://substrate.office.comN	0%	Avira URL Cloud	safe	
http://https://substrate.office.comV	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com)n0	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://outlook.office.com&	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.8.146.139/fhfty/SKWR8YXON-RX9R4781JWMO3UUH0NGDBO/-f	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://shell.suite.office.com:1443	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://autodiscover-s.outlook.com/	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	WINWORD.EXE, 00000000.00000000.289192987.000000000D1FB000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.266167152.000000000D1FB000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize0_	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.entity.	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizeB%	WINWORD.EXE, 00000000.00000000.300743360.000000000DA70000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267141726.000000000DA70000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://messaging.action.office.com/setuseraction16A	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://outlook.office365.com/d0	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://rpsticket.partnerservices.getmicrosoftkey.com	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizePt	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://settings.outlook.comS	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.8.146.139/fhfty/SKWR8YXON-RX9R4781JWMO3UUH0NGDBO/-f71USERNAME=userUSERPROFILE=C:	WINWORD.EXE, 00000000.00000000.291653462.000000000DCF7000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267974065.000000000DCF7000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	WINWORD.EXE, 00000000.00000000.299025740.000000000D0BF000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.265671015.000000000D0BF000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech)	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://api.aadrm.com/	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.o365filtering.com/Ep	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://prod.mds.office.com/mds/api/v1.0/clientmodeldirectoryTV	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	WINWORD.EXE, 00000000.00000000.299221788.000000000D11D000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.265756794.000000000D11D000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=ImmersiveApp	WINWORD.EXE, 00000000.00000000.300743360.000000000DA70000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267141726.000000000DA70000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://api.microsoftstream.com/api/	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://cr.office.com	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://web.microsoftstream.com/video/#rF	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizeQu	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false	• URL Reputation: safe	unknown
http://https://my.microsoftpersonalcontent.com	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false	• URL Reputation: safe	unknown
http://45.8.146.139/fhfty/SKWR8YXON-RX9R4781JWMO3UUH0NGDBO/-fOOC:	WINWORD.EXE, 00000000.00000000.299992544.000000000D27B000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false	• URL Reputation: safe	unknown
http://https://messaging.engagement.office.com/	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://onedrive.live.com/embed?i	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/.	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://graph.ppe.windows.net/%	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://www.odwebp.svc.ms	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false	• URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://clients.config.office.net/ds	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://web.microsoftstream.com/video/	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false	• URL Reputation: safe	unknown
http://https://substrate.office.comp	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://graph.windows.net	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizeR$	WINWORD.EXE, 00000000.00000000.300743360.000000000DA70000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267141726.000000000DA70000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dataservice.o365filtering.com/ym	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://login.windows.net/common/oauth2/authorize/_	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://augloop.office.com/v2(	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://dataservice.o365filtering.com2p7	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ncus.contentsync.	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false	• URL Reputation: safe	unknown
http://https://o365auditrealtimeingestion.manage.office.com/api/userauditrecord8	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://substrate.office.comN	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://login.windows.net/common/oauth2/authorize&zJ	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizeA$	WINWORD.EXE, 00000000.00000000.300743360.000000000DA70000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267141726.000000000DA70000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://outlook.office365.com/autodiscover/autodiscover.jsonV	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	WINWORD.EXE, 00000000.00000000.289192987.000000000D1FB000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.266167152.000000000D1FB000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://weather.service.msn.com/data.aspx	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://substrate.office.comP	WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		unknown
http://https://login.windows.net/common/oauth2/authorizeOt	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://substrate.office.comV	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.o365filtering.com)n0	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://substrate.office.comW	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://login.windows.net/common/oauth2/authorizeb	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://wus2.contentsync.	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false	• URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorized	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.windows.net/common/oauth2/authorize~t	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://globaldisco.crm.dynamics.comom	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/ios	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizep$	WINWORD.EXE, 00000000.00000000.300743360.000000000DA70000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267141726.000000000DA70000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizeX	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizeY	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://excel.uservoice.com/forums/304936-excel-for-mobile-devices-tablets-phones-androidv.	WINWORD.EXE, 00000000.00000000.300743360.000000000DA70000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267141726.000000000DA70000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://o365auditrealtimeingestion.manage.office.com	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://outlook.office.com&	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://outlook.office365.com/api/v1.0/me/Activities	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/android/policies	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizeR	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizeS	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://analysis.windows.net/powerbi/apiU	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://entitlement.diagnostics.office.com	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizeW	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizeH	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office.com/	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/mack	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://storage.live.com/clientlogs/uploadlocation	WINWORD.EXE, 00000000.00000000.300743360.000000000DA70000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267141726.000000000DA70000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizeN	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizeB	WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorize;u%	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizeC	WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, 2687EECC-4F43-442C-AA69-7E12CA414CA2.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorizeF	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorizeq%	WINWORD.EXE, 00000000.00000000.300743360.000000000DA70000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267141726.000000000DA70000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://login.windows.net/common/oauth2/authorize;	WINWORD.EXE, 00000000.00000000.290169035.000000000DAFD000.00000004.00000001.00020000.00000000.sdmp, WINWORD.EXE, 00000000.00000000.267363427.000000000DAFD000.00000004.00000001.00020000.00000000.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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682606
Start date and time:	2022-08-11 18:57:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	valliant.document.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:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal80.expl.winDOC@3/11@0/2
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, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.32.24, 52.109.88.39, 52.109.88.37, 20.189.173.21
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, 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, onedsblobprdwus16.westus.cloudapp.azure.com, nexus.officeapps.live.com, displaycatalog.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
18:59:16	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_2bb258ba8dfc7dfa5c63c367cd77571e93c8305c_5f94c319_0841aa39\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):	1.6333582842029912
Encrypted:	false
SSDEEP:	192:hIrTZNvH7OHSTjjKYbVrPR/wttRJp/u7snS274Itu0:qrnv7OHSTjdRY3RJp/u7snX4Itu
MD5:	AC6EEF4FA3F48FD8D1EFE0C61C9404E6
SHA1:	2CF87F041CDFFFC1E6FFA75C936F0CC726F62460
SHA-256:	CAB32F91FCE62092D1FB0AEAF4E7124F7BB45686540A1C5AD1BA0088843FAF79
SHA-512:	98E86550AA14AFCAD490EBD5EA37C85A9FE25D535A44BBF3B72C54774EB7A8C34C722A0AE4C473D992EAEDCF506DBFF97A5100721D9FB0A66E4113BBFBDCFCFD
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.=.1.3.3.0.4.7.4.3.1.5.0.1.0.3.4.9.4.5.....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.=.1.3.3.0.4.7.4.3.1.5.2.8.5.3.4.8.6.7.....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.=.6.b.b.4.5.e.e.c.-.f.2.d.2.-.4.5.c.c.-.a.6.5.b.-.2.1.1.d.a.9.b.3.6.a.2.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.7.6.5.4.a.8.7.-.0.5.8.3.-.4.9.c.4.-.8.9.9.a.-.d.0.6.7.5.e.1.5.a.3.7.5.....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.b.5.c.-.0.0.0.1.-.0.0.1.d.-.2.6.8.b.-.8.2.0.8.e.f.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\WER8FDB.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Aug 12 01:59:11 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	306553
Entropy (8bit):	2.6527023369025584
Encrypted:	false
SSDEEP:	1536:VjL4UE6KH2bnsSiG0xty9CF+AI3Sx3w5CjtyWnnZj7p5tVvQGYehT:VzE6F9rctymoSLjtJZj7LhYehT
MD5:	0E6F88ACF9FA9C8B3CEBC90B5A551E09
SHA1:	54C2E1F48112E383766187CC025B0514D164BDDD
SHA-256:	79433D518689C5DF597DD314CB17529E505D73D24DF3C5D272763DDB50583745
SHA-512:	384F8DCC7C55BE7FFDA837B0DFA261B0000EBD119EADD4DD9F8D788A898E37C9C27030C074BC347BCE32E3A9C69B1FF6580E403DCBE57B85AB053F97A82AE457
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....b.....:.....F.....`.....8.....T.....DH.....0J.....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\WER980A.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):	8348
Entropy (8bit):	3.709926400831255
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiUC6k6YTaSUOggmf7SDTCpDK89b9isf1/m:RrlsNip6k6YOSUOggmf7SDo9hfQ
MD5:	E716E2FE7257341D1DE1B62C1430DA3F
SHA1:	243865FDF0A967BED04F022CA74D75D759579C19
SHA-256:	E87D4EC52A44A06A2DD0B71185095219B8E14CEDFAC16EB4CE013942FDF125B8
SHA-512:	6559307BB2B4DDCE13B6D41FCC37C9ECE196000105B9D938356256E760F8D1DA41F40C0CC9F34C9ECB633878A2CFB3111997196331D801F1AC7DFC64E7455DC
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.>.2.9.0.8.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9962.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):	4.5295296067639015
Encrypted:	false
SSDEEP:	48:cvIwSD8zsaJgtWI9jrWgc8sqYj/8fm8M4Jx7FNV+q88U58UvFeVqd:uITfoEagrsqYwJ/UTvoqd
MD5:	0013CEC3EB6831E813B3A8FA514E3AAD
SHA1:	1C70C828985F6ED1FE68B5405238B0F38FBFAB71
SHA-256:	DA9A2C5C4613EBFE4BAF57447901018DA53F1E774A8EEAE1C1979AF4A3C7DEC5
SHA-512:	5E36622299DF4C146DB647F73718E452EB7C9995ACBFB33C2B656DC0DDC3BB85B16AE4B0F7D7B0D474A86F7E31004F800B24414C4E41B2DBBB20D3FC54993A1A
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="1643709" />.. <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\2687EECC-4F43-442C-AA69-7E12CA414CA2

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):	5.358162199787249
Encrypted:	false
SSDEEP:	1536:gcQW/gxgB5BQguwN/Q9DQe+zQTk4F77nXmvid3XxVETLKz61:T1Q9DQe+zuXYr
MD5:	621F80E05552B3ECF353464BC4E9B294
SHA1:	1E83E9E01E369F73C7C858E0ACC9FBD90BFF127D
SHA-256:	D38400A3A86BD0DD654C844D8F867F49C6E428661BC88F9D8B335E2C0D7BC02B
SHA-512:	AD6FE0EF23749D635FE1B3A6B57BA1013B735026F921CECAFD0026FE4E3645CB45C2FB8AAF07B0C8130111A4DC6549D49561A08DA05B477543DE93B16E7770AE
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="2022-08-11T16:58:39">.. 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:	24CDCCA259970B669949BD197AA55FD6E05D91B53A05984D3EBB3B219B6D26BDD67165967F1C8960D55E517D7AC46E1E515DD6E5C45DE4923F2FB1B1A98BCI 22
Malicious:	false
Reputation:	low
IE Cache URL:	http://45.8.146.139/fhfty/SKWR8YXON-RX9R4781JWMO3UUH0NGDBO/-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\yD159.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**
Reputation:	low
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\index.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	115
Entropy (8bit):	4.643502388640172
Encrypted:	false
SSDEEP:	3:bDuMJlLWRBKHIALRlj9TLBCmX10JFRBKHIALRlj9TLBCv:bCAeB7ALr9HBSbB7ALr9HBs
MD5:	3CB5E2D635FB7887310A38F71EA6ADDD
SHA1:	3B07E380CE6B8C0E07368C0CF952F496E21ADFD7
SHA-256:	54314B21351BEC27FE14EB4EA2EC466892A9B1B433C85699C6920071C9D21871
SHA-512:	9676D4A3881D1D7D41D56472BC45083BE30382DED70C564B69277826AF4A8B04B46E684C436ED932C679414319C0F8CD01D1CA9E210F2A54A663A7B964D4592
Malicious:	false
Preview:	[folders]..Templates.LNK=0..valliant.document.08.11.2022.doc.LNK=0..[doc]..valliant.document.08.11.2022.doc.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\valliant.document.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 15:31:42 2022, mtime=Fri Aug 12 00:58:40 2022, atime=Fri Aug 12 00:58:35 2022, length=2221348, window=hide
Category:	dropped
Size (bytes):	1145
Entropy (8bit):	4.699008530144123
Encrypted:	false
SSDEEP:	12:8TnHckRUVuElPCH2bQept1Yv0hX+WpQQzps0gjAU/4B789LtH0ID9l5v4t2Y+xl/:8zHzfepfhLQQt6AUc89fDXH7aB6m
MD5:	D68B1F3E3D0554FA7E1A874C499BD3CF
SHA1:	D492C29EBCC85549BC4ABBFDDE00832D29A58364
SHA-256:	4DC8E47EB7BDE47F406129F5670874BE7CA488A4AD50A1B60F0A535D77DF2E5C
SHA-512:	42753C655E1A3DB8D2E99136D762D42FCF0ADD441585714A5091FA8D17C9F4B22DAD635A450C0823AF11EFA5A5527C786CAFBA1839551F272F59F220CC130AF
Malicious:	**true**
Preview:	L.....F.... ....zm..3....K.....*....$.!.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...UK.....:.....q\|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....hT....user.<.....Ny..UK.....S.....mK..h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..UK.....Y.....>.....t.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.$.!..UR. .VALLIA~1.DOC..r.....hT...UR.....h.....g.v.a.l.l.i.a.n.t...d.o.c.u.m.e.n.t...0.8...1.1...2.0.2.2...d.o.c.....f.....-.....e.....>.S.....C:\Users\user\Desktop\valliant.document.08.11.2022.doc..7.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.v.a.l.l.i.a.n.t...d.o.c.u.m.e.n.t...0.8...1.1...2.0.2.2...d.o.c.....:.,.LB.)...As...`.....X.....992547.....!a..%.H.VZAj.....-..!a..%.H.VZAj.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1657932117250045
Encrypted:	false
SSDEEP:	3:Rl/ZdxiDyvtlliVX9lqKYistr:RtZziDOil2sR
MD5:	23A678C8A7437AA29240B630EDC73E46
SHA1:	2D47627B182956BFD3B6001F05E6598F87049A91
SHA-256:	31B3A272B06650F92E6076C59E89ADA8E5E567ECE563EE8D5D890ACBDADE5104
SHA-512:	663F4931E8A9A8BC685EA6F6B2F58AC9EFF4242B845DE184B70AE02E99716AFA80226179554500C5FAEE6C11E0E156E77209AEB86ECBB8C313390B732C2C343A
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....N.....9.J.....$.....6C.....=.v.....T...

C:\Users\user\Desktop\~$lliant.document.08.11.2022.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1657932117250045
Encrypted:	false
SSDEEP:	3:Rl/ZdxiDyvtlliVX9lqKYistr:RtZziDOil2sR
MD5:	23A678C8A7437AA29240B630EDC73E46
SHA1:	2D47627B182956BFD3B6001F05E6598F87049A91
SHA-256:	31B3A272B06650F92E6076C59E89ADA8E5E567ECE563EE8D5D890ACBDADE5104
SHA-512:	663F4931E8A9A8BC685EA6F6B2F58AC9EFF4242B845DE184B70AE02E99716AFA80226179554500C5FAEE6C11E0E156E77209AEB86ECBB8C313390B732C2C343A
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....N.....9.J.....$.....6C.....=.v.....T...

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993464543538008
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:	valliant.document.08.11.2022.doc
File size:	2316502
MD5:	cadb9d5ed47b8df81a2addefed302a03
SHA1:	f7197fa991510f99f25af2b502c40d3b48d1abbc
SHA256:	9cb01729327bd958e32aa9481d5a81303627ab7a59b9ae134fb6600ef4e5b680
SHA512:	1b5ed9721c8d1aed9d09a850cb43afd6d756bbf6957ca6d8321c1fb5ea89a88a448f0aaa60348a70e30eda299c554619961c89b12888ea2ad6a6a5d058a54b07
SSDEEP:	49152:7t3L6IYFlSbzCFelOb0h5CZTsXG97qRbET6DLZ6dGbrG5j:BPYYgelO9T6G97qVg6DLZ6dGbyh
TLSH:	6DB533ED89E8E561F1433E32380557F3A45410D6EA5AC84A30C6FFC197962BB36E4F92
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/682606/sample/valliant.document.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: 2826

General

Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2826
Data ASCII:	. . A t t r i b u t . e V B _ N a m . e = " T h i . s D o c u m e n . t " . . . B a s . . 1 N o r m a l . . . V G l o b a l ! . S p a c . l F a . l s e . J C r e a . t a b l . . P r e d e c l a . . I d . . # T r u . " E x p . o s e . . T e m p . l a t e D e r i . v . $ C u s t o m l i z C . P . . . . . D . ? P t r S a . f e F u n c t . i o n > . . . . L . i b " u s e r . 3 2 " A l i a . s " S e t T i . m e r " (B y 8 V a l . . . . A s L o n g . , ... 3 . 9 . .
Data Raw:	01 fa 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:	5.261233037013654
Base64 Encoded:	True
Data ASCII:	I D = " { 8 B 8 0 C 6 E 6 - B 7 5 8 - 4 1 8 F - A 2 4 D - 0 6 C 5 2 D 3 9 3 F 8 5 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 0 5 0 7 D 9 E 6 D B E F D F E F D F E F D F E F D F " . . D P B = " 0 A 0 8 D 6 E 1 D A E 2 D A E 2 D A " . . G C = " 0 F 0 D D 3 E C D D F 4 E 3 F 5 E 3 F 5 1 C " . . . . [H o s t E x t e n d e r I n f
Data Raw:	49 44 3d 22 7b 38 42 38 30 43 36 45 36 2d 42 37 35 38 2d 34 31 38 46 2d 41 32 34 44 2d 30 36 43 35 32 44 33 39 33 46 38 35 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 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:	T h i s D o c u m e n t . 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
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: 5100	
General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	5100
Entropy:	1.9259173726592043
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 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 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 50 00 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:	2.7004238887086345
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . x . . . . . ` . . . . . . . . . . . . . . p . . . . . . . . . . . . . . . . . ! . . . . . . . . A . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . ` . . . . , . . p . . . . A . . . . a . . . . P . . . . \\ . . p
Data Raw:	72 55 40 00 00 00 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 1a 00 00 00 00 00 00 00 11 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 c1 08 00 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 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:	6.3067050501427175
Base64 Encoded:	True
Data ASCII:	. . . . 0 . . . . . . H . . . . P r o j e c t . Q . (. . @ . . . . . = ... 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 d3 40 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 18:58:45.151184082 CEST	49741	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:58:45.255310059 CEST	80	49741	45.8.146.139	192.168.2.3
Aug 11, 2022 18:58:45.255506992 CEST	49741	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:58:45.272706032 CEST	49741	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:58:45.376708984 CEST	80	49741	45.8.146.139	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 18:58:45.396755934 CEST	80	49741	45.8.146.139	192.168.2.3
Aug 11, 2022 18:58:45.396877050 CEST	49741	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:58:50.402072906 CEST	80	49741	45.8.146.139	192.168.2.3
Aug 11, 2022 18:58:50.402266979 CEST	49741	80	192.168.2.3	45.8.146.139
Aug 11, 2022 18:59:23.421643019 CEST	49741	80	192.168.2.3	45.8.146.139

HTTP Request Dependency Graph

- 45.8.146.139

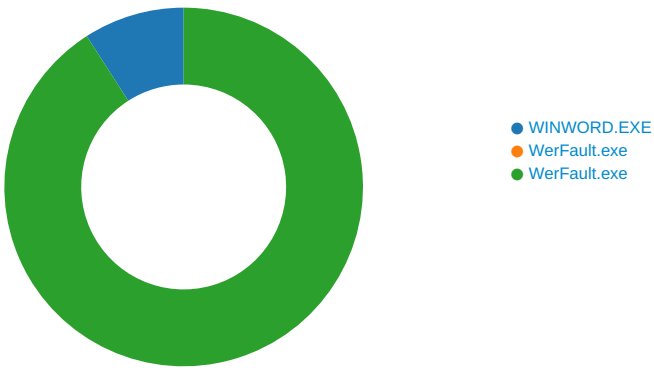
HTTP Packets

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 18:58:45.272706032 CEST	1179	OUT	GET /fhfty/SKWR8YXON-RX9R4781JWMO3UUH0NGDBO/-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 18:58:45.396755934 CEST	1180	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 16:58:45 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: **2908**, Parent PID: **756**

General

Target ID:	0
Start time:	18:58:36
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:	0x1390000
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\tstC08C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstC08D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstC0BD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstC0BE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	65B82F42	unknown
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	659F977C	unknown
C:\Users\user\AppData\Local\Temp\yD159.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14DE46AB	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	14DE6626	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	14DE6626	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	14DE6626	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	14DE6626	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	14DE6626	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	14DE6626	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	14DE6626	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	14DE6626	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	14DE6626	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	14DE6626	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	14DE6626	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	14DE6626	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\yD159.tmp.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14DE6626	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tstC08C.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstC08D.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstC0BD.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\tstC0BE.tmp	success or wait	1	65B82F42	unknown
C:\Users\user\AppData\Local\Temp\yD159.tmp	success or wait	1	14DE4702	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	14DE6626	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\yD159.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	14DE6626	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\valliant.document.08.11.2022.doc	unknown	14	success or wait	2	65B82FF3	unknown
C:\Users\user\Desktop\valliant.document.08.11.2022.doc	unknown	4	success or wait	16	65B8253D	unknown
C:\Users\user\AppData\Local\Temp\yD159.tmp.dll	unknown	4096	success or wait	1	14E514C0	ReadFile
C:\Users\user\AppData\Local\Temp\yD159.tmp.dll	unknown	4096	end of file	1	14E514C0	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	65938A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	65938A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	65938A84	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: **1928**, Parent PID: **2908**

General

Target ID:	17
Start time:	18:59:08
Start date:	11/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2908 -s 4128
Imagebase:	0xbf0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: **2072**, Parent PID: **2908**

General

Target ID:	18
Start time:	18:59:08
Start date:	11/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2908 -s 4132
Imagebase:	0xbf0000
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	6F751717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9962.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9962.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F74497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_WINWORD.EXE_2bb258ba8dfc7dfa5c63c367cd77571e93c8305c_5f94c319_0841aa39	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_WINWORD.EXE_2bb258ba8dfc7dfa5c63c367cd77571e93c8305c_5f94c319_0841aa39\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F74497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9962.tmp	success or wait	1	6F74497A	unknown
C:\Users\user\AppData\Local\Temp\{8011A935-294F-4F63-BF68-112F881F16E0} - OProcSessId.dat	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9962.tmp.xml	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER406E.tmp.csv	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER408E.tmp.txt	success or wait	1	6F74497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 fd fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	19144	6	00 00 00 00 00 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.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 5c 0b 00 00 f3 fd 62 03 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 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 00	UBJGenuineIntelWT\b0Pacific Standard TimePacific Daylight Time	success or wait	1	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	23952	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 74 fd 14 fd 70 fd 14 64 01 0f 01 00 00 00 00 fd 5e 4d 0b fd 5e 4d 0b 58 01 0f 01 fd 68 fd 14 23 00 00 00 06 02 21 00 68 fd 0e 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++tpd^M^MXh#!h+	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	1632	168	fd 07 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 fd 5e 4d 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 00 00 fd 02 00 00 fd 5d 00 00	h^M]	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	39704	20	1d 01 00 00 38 fd 0d 00 00 00 00 04 00 00 00 fd 00 00	8	success or wait	285	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	44268	4	74 16 19 6b	tk	success or wait	284	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	239671	4	60 fd fd 69	`i	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	1800	4	15 00 00 00		success or wait	21	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	24668	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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 64 01 0f 01 00 00 00 00 fd fd fd fd fd fd fd 58 01 0f 01 fd 68 fd 14 23 00 00 00 06 02 21 00 68 fd 0e 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++dXh#!h+	success or wait	21	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	2764	48	34 05 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 60 fd 00 00 00 00 00 78 fd fd 14 00 00 00 00 fd 03 00 00 0b fd 03 00 fd 02 00 00 4c fd 00 00	4 `xL	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	2824	4	fd 00 00 00		success or wait	141	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	19150	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	17948	120	00 00 10 65 00 00 00 00 00 50 38 00 fd 50 38 00 fd 79 06 00 22 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 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	eP8P8y"[BB?+@A	success or wait	18	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	23372	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	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	18476	668	00 00 fd 65 00 00 00 00 00 fd 03 00 fd 0e 04 00 55 00 fd 59 74 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 fd fd 02 00 00 00 00 00 70 fd 02 00 00 00 00 2e fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 1d fd 03 00 00 00 00 00 2e fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 46 1a 00 00 00 00 00 35 fd 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 05 00 00 00 00 00 00 fd fd 5f 55 00 00 00 00 00 65 fd fd 1c 00 00 00 00 00 53 7a fd 20 00 00 00 00 00 fd fd fd 01 00 00 00 00 fd fd 00 00 1a 0d 01 00 3a 27 07 00 fd 17 0a 00 35 fd 05 00 06 7f 15 00 fd fd 05 00 4a 5c 44 00 2e fd 01 00 fd fd 17 00 00 00 00 00 fd 2d 00 7d fd 04	eUYt]Zbp..F5@_UeSz :'5J\D.-}	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	239675	66878	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 00 00 00 28 00 00 00 57 00 61 00 69	KeyEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(Wai	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FDB.tmp.dmp	32	120	03 00 00 00 fd 03 00 00 08 07 00 00 04 00 00 00 fd 3b 00 00 08 0b 00 00 0e 00 00 00 fd 01 00 00 fd 46 00 00 05 00 00 00 fd 11 00 00 18 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 0c 04 00 15 00 00 00 fd 01 00 00 44 48 00 00 16 00 00 00 fd 00 00 00 30 4a 00 00	;F`8TDH0J	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 32 00 39 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>2908</Pid>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1070	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1074	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1168	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1172	2	09 00		success or wait	2	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1176	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 36 00 32 00 39 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>36298</Uptime>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 32 00 37 00 31 00 31 00 38 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>542711808</PeakVirtualSize>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 32 00 36 00 34 00 36 00 32 00 37 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>542646272</VirtualSize>	success or wait	1	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 32 00 39 00 34 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>52941</PageFaultCount>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1688	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1692	2	09 00		success or wait	3	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 33 00 30 00 36 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>136306688</PeakWorkingSetSize>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1798	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1802	2	09 00		success or wait	3	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 33 00 30 00 36 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>136306688</WorkingSetSize>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1892	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	1896	2	09 00		success or wait	3	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2016	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2020	2	09 00		success or wait	3	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 35 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>910568</QuotaPagedPoolUsage>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2124	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2128	2	09 00		success or wait	3	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 36 00 30 00 39 00 30 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>609016</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2260	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2264	2	09 00		success or wait	3	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 36 00 30 00 38 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>608880</QuotaNonPagedPoolUsage>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2380	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2384	2	09 00		success or wait	3	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 37 00 37 00 37 00 34 00 38 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>77774848</PagefileUsage>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2468	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2472	2	09 00		success or wait	3	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 37 00 39 00 34 00 32 00 37 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>77942784</PeakPagefileUsage>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2572	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2576	2	09 00		success or wait	3	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 37 00 37 00 37 00 37 00 34 00 38 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>77774848</PrivateUsage>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2656	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2660	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2710	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2714	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2748	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2752	2	09 00		success or wait	3	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2798	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2802	2	09 00		success or wait	4	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2838	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2842	2	09 00		success or wait	4	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3032	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 38 00 37 00 30 00 30 00 32 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5870021</Uptime>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3080	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3084	2	09 00		success or wait	4	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3394	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3398	2	09 00		success or wait	5	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3482	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3486	2	09 00		success or wait	5	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 38 00 39 00 36 00 39 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>8969</PageFaultCount>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3570	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3574	2	09 00		success or wait	5	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 32 00 31 00 39 00 36 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>24219648</PeakWorkingSetSize>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3682	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3686	2	09 00		success or wait	5	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 30 00 39 00 32 00 36 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>24092672</WorkingSetSize>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3778	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3782	2	09 00		success or wait	5	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 37 00 35 00 35 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>475576</QuotaPeakPagedPoolUsage>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3906	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	3910	2	09 00		success or wait	5	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 33 00 39 00 31 00 39 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>439192</QuotaPagedPoolUsage>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4018	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4022	2	09 00		success or wait	5	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 37 00 36 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>24760</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4156	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4160	2	09 00		success or wait	5	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 33 00 39 00 32 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>23392</QuotaNonPagedPoolUsage>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4278	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4282	2	09 00		success or wait	5	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.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 36 00 36 00 32 00 34 00 36 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>9662464</PagefileUsage>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4368	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4372	2	09 00		success or wait	5	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4382	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 37 00 38 00 35 00 33 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>9785344</PeakPagefileUsage>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4474	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4478	2	09 00		success or wait	5	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4488	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 36 00 36 00 32 00 34 00 36 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>9662464</PrivateUsage>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4560	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4564	2	09 00		success or wait	4	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4572	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4618	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4622	2	09 00		success or wait	3	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4628	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4670	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4674	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4678	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4716	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4764	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4802	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4806	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4810	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4872	4	0d 00 0a 00		success or wait	8	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4876	2	09 00		success or wait	16	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	4880	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	5534	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	5538	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	5540	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	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	5580	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	5584	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	5586	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	5624	4	0d 00 0a 00		success or wait	6	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	5628	2	09 00		success or wait	12	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	5632	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6186	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6190	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6192	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6232	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6236	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6238	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6276	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6280	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6284	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6378	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6382	2	09 00		success or wait	2	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6386	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 71 00 75 00 73 00 61 00 6a 00 6e 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>qusajn, Inc.</SystemManufacturer>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6492	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6496	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6500	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 71 00 75 00 73 00 61 00 6a 00 6e 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>qusajn7,1</SystemProductName>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6596	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6600	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6604	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6724	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6728	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6732	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 36 00 39 00 38 00 35 00 35 00 39 00 38 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1606985598</OSInstallDate>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6814	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6818	2	09 00		success or wait	2	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6822	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6924	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6928	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	6932	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7000	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7004	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7006	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7046	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7050	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7052	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7086	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7090	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7094	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7190	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7194	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7196	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	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7232	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7236	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7238	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7262	4	0d 00 0a 00		success or wait	3	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7266	2	09 00		success or wait	6	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7270	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7522	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7526	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7528	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7554	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7558	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7560	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 39 00 3a 00 31 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-08-12T01:59:12Z">	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7660	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7664	2	09 00		success or wait	2	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7668	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 32 00 38 00 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 39 00 30 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 39 00 31 00 35 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 39 00 31 00 35 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 00 3d 00 22	<Process AsId="283" PID="2908" UptimeMS="9156" TimeSinceCreationMS="9156" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7930	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7934	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7938	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7958	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7962	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	7964	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	8002	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	8006	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	8008	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	8046	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	8050	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	8054	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 62 00 62 00 34 00 35 00 65 00 65 00 63 00 2d 00 66 00 32 00 64 00 32 00 2d 00 34 00 35 00 63 00 63 00 2d 00 61 00 36 00 35 00 62 00 2d 00 32 00 31 00 31 00 64 00 61 00 39 00 62 00 33 00 36 00 61 00 32 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>6bb45eec-f2d2-45cc-a65b-211da9b36a23</Guid>	success or wait	1	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	8152	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	8156	2	09 00		success or wait	2	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	8160	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 39 00 3a 00 31 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-08-12T01:59 :12Z</CreationTime>	success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	8258	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	8262	2	09 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	8264	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	8304	4	0d 00 0a 00		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER980A.tmp.WERInternalMetadata.xml	8308	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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9962.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	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_WINWORD.EXE_2bb258ba8dfc7dfa5c63c367cd77571e93c8305c_5f94c319_0841aa39\Report.wer	0	2	fd fd		success or wait	1	6F74497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_WINWORD.EXE_2bb258ba8dfc7dfa5c63c367cd77571e93c8305c_5f94c319_0841aa39\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	6F74497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_WINWORD.EXE_2bb258ba8dfc7dfa5c63c367cd77571e93c8305c_5f94c319_0841aa39\Report.wer	22882	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 32 00 30 00 34 00 38 00 36 00 35 00 36 00 30 00 35 00	MetadataHash=204865605	success or wait	1	6F74497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	success or wait	1	6F7636BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6F761FB2	RegCreateKeyExW
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F7443D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	ProgramId	unicode	00069598d3287916f374a839556055d0342700000000	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	FileId	unicode	0000404de7544598f08723ea1f13c0724aef5ac5af34	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	LowerCaseLongPath	unicode	c:\program files (x86)\microsoft office\office16\winword.exe	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	LongPathHash	unicode	winword.exe|597535ad	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	Name	unicode	winword.exe	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	Publisher	unicode	microsoft corporation	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	Version	unicode	16.0.4993.1001	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	BinFileVersion	unicode	16.0.4993.1001	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	BinaryType	unicode	pe32_i386	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	ProductName	unicode	microsoft office 2016	success or wait	1	6F7636BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	ProductVersion	unicode	16.0.4993.1001	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	LinkDate	unicode	03/21/2020 12:12:22	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	BinProductVersion	unicode	16.0.4993.0	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	Size	B	18 91 1D 00 00 00 00 00	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	Language	dword	0	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	IsPeFile	dword	1	success or wait	1	6F7636BF	unknown
\REGISTRY\A\{9f411095-9d39-752b-f6d7-827ebc15715b}\Root\InventoryApplicationFile\winword.exe|597535ad	IsOsComponent	dword	0	success or wait	1	6F7636BF	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 DE 14 02 00 00 00 00 00 00 00 DF 5E 4D 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	success or wait	1	6F761FE8	RegSetValueExW

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

Disassembly

No disassembly