ID: 701320
Sample Name: 12-09-2022 S#U0130PAR#U0130#U015e.docx.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:44:10
Date: 12/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

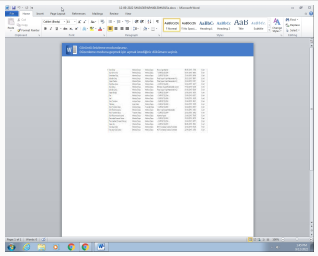
Windows Analysis Report

12-09-2022 S#U0130PAR#U0130#U015e.docx.doc

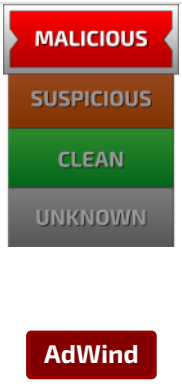
Overview

General Information

Sample Name:	12-09-2022 S#U0130PAR#U0130#U015e.docx.doc
Analysis ID:	701320
MD5:	7e8133cf5f56adc..
SHA1:	2cc6471245901e..
SHA256:	7859fd95c60a0d..
Tags:	doc
Infos:	



Detection



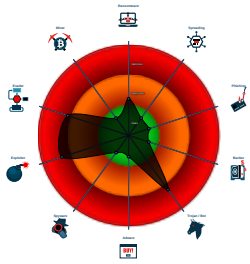
AdWind

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

Signatures

- Document exploit detected (creates…
- Multi AV Scanner detection for subm…
- Yara detected AdWind RAT
- Document contains OLE streams w…
- Document exploit detected (process…
- Queries sensitive BIOS Information…
- Found inlined nop instructions (likely…
- May sleep (evasive loops) to hinder…
- Detected potential crypto function
- Queries sensitive processor informa…
- Creates a process in suspended mo…
- Queries sensitive Operating System…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1216 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - javaw.exe (PID: 1952 cmdline: "C:\Program Files\Java\jre1.8.0_121\bin\javaw.exe" -jar "C:\Users\user\AppData\Local\Temp\a0v2H8.jar" MD5: 7F0467C3AA5BDAF44BBC824AC81359D0)
    - WMIC.exe (PID: 2452 cmdline: wmic CPU get ProcessorId MD5: FD902835DEAEF4091799287736F3A028)
    - WMIC.exe (PID: 2308 cmdline: wmic bios get serialnumber MD5: FD902835DEAEF4091799287736F3A028)
    - WMIC.exe (PID: 772 cmdline: wmic csproduct get name MD5: FD902835DEAEF4091799287736F3A028)
    - WMIC.exe (PID: 1916 cmdline: wmic csproduct get UUID MD5: FD902835DEAEF4091799287736F3A028)
  - javaw.exe (PID: 1316 cmdline: "C:\Program Files\Java\jre1.8.0_121\bin\javaw.exe" -jar "C:\Users\user\AppData\Local\Temp\a0v2H8.jar" MD5: 7F0467C3AA5BDAF44BBC824AC81359D0)
    - WMIC.exe (PID: 2016 cmdline: wmic CPU get ProcessorId MD5: FD902835DEAEF4091799287736F3A028)
    - WMIC.exe (PID: 2344 cmdline: wmic bios get serialnumber MD5: FD902835DEAEF4091799287736F3A028)
    - WMIC.exe (PID: 316 cmdline: wmic csproduct get name MD5: FD902835DEAEF4091799287736F3A028)
    - WMIC.exe (PID: 2496 cmdline: wmic csproduct get UUID MD5: FD902835DEAEF4091799287736F3A028)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.1107491922.00000000D7403000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AdWind_2	Yara detected AdWind RAT	Joe Security	
00000003.00000002.1046522557.00000000D747C000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AdWind_2	Yara detected AdWind RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000002.1108130731.00000000D7479000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AdWind_2	Yara detected AdWind RAT	Joe Security	
00000003.00000002.1045659100.00000000D7407000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AdWind_2	Yara detected AdWind RAT	Joe Security	
Process Memory Space: javaw.exe PID: 1952	JoeSecurity_AdWind_2	Yara detected AdWind RAT	Joe Security	
Click to see the 1 entries				

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

Software Vulnerabilities

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

System Summary

Document contains OLE streams which likely are hidden ActiveX objects

Malware Analysis System Evasion

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Stealing of Sensitive Information

Yara detected AdWind RAT

Remote Access Functionality

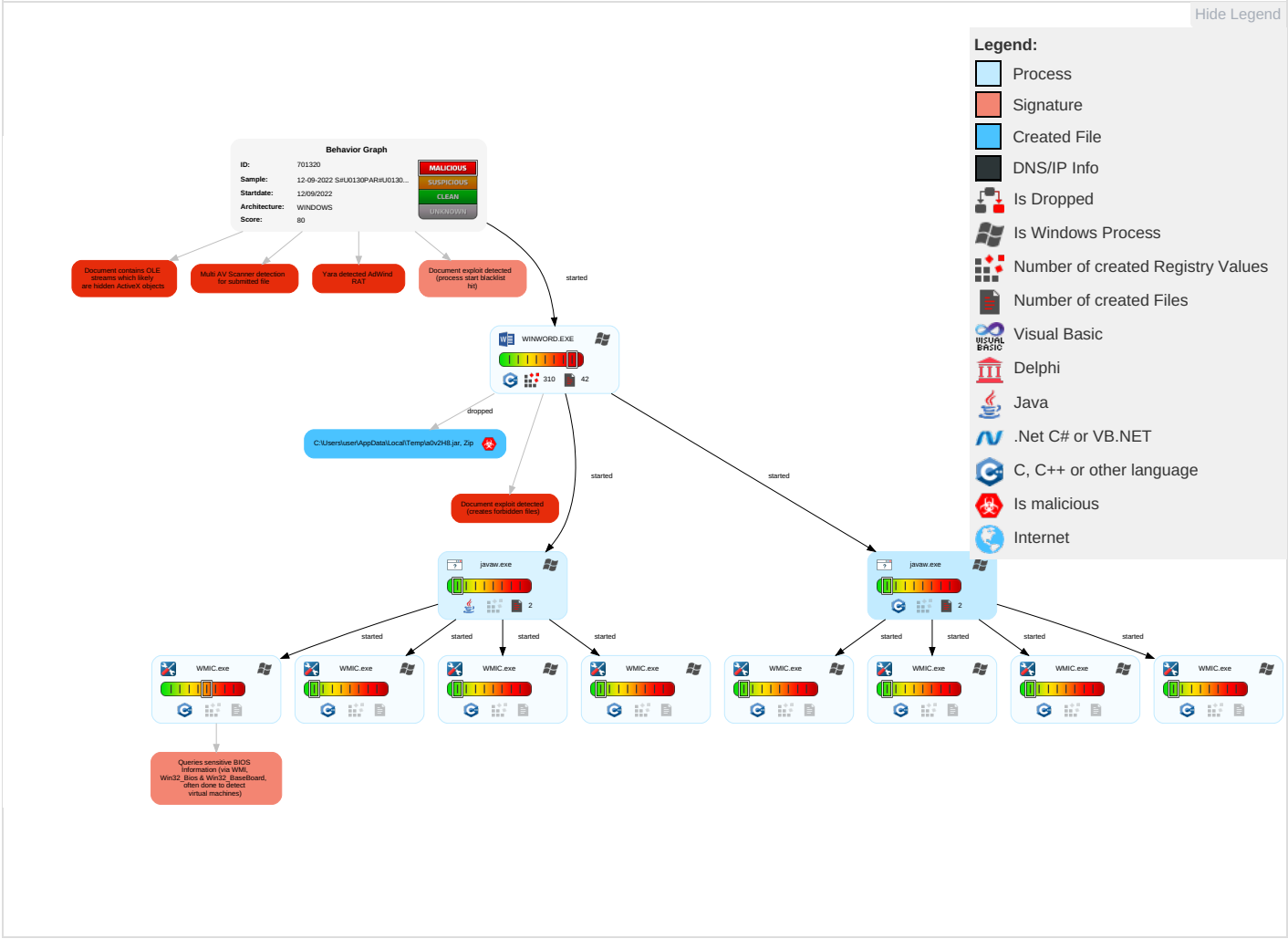
Yara detected AdWind RAT

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

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 1 Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Masquerading	OS Credential Dumping	2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	3 Virtualization/Sandbox Evasion	LSASS Memory	3 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 1 4 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	1 1 Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

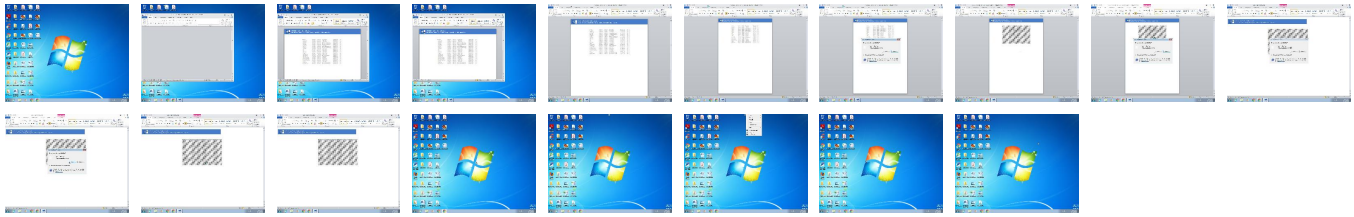
Behavior Graph

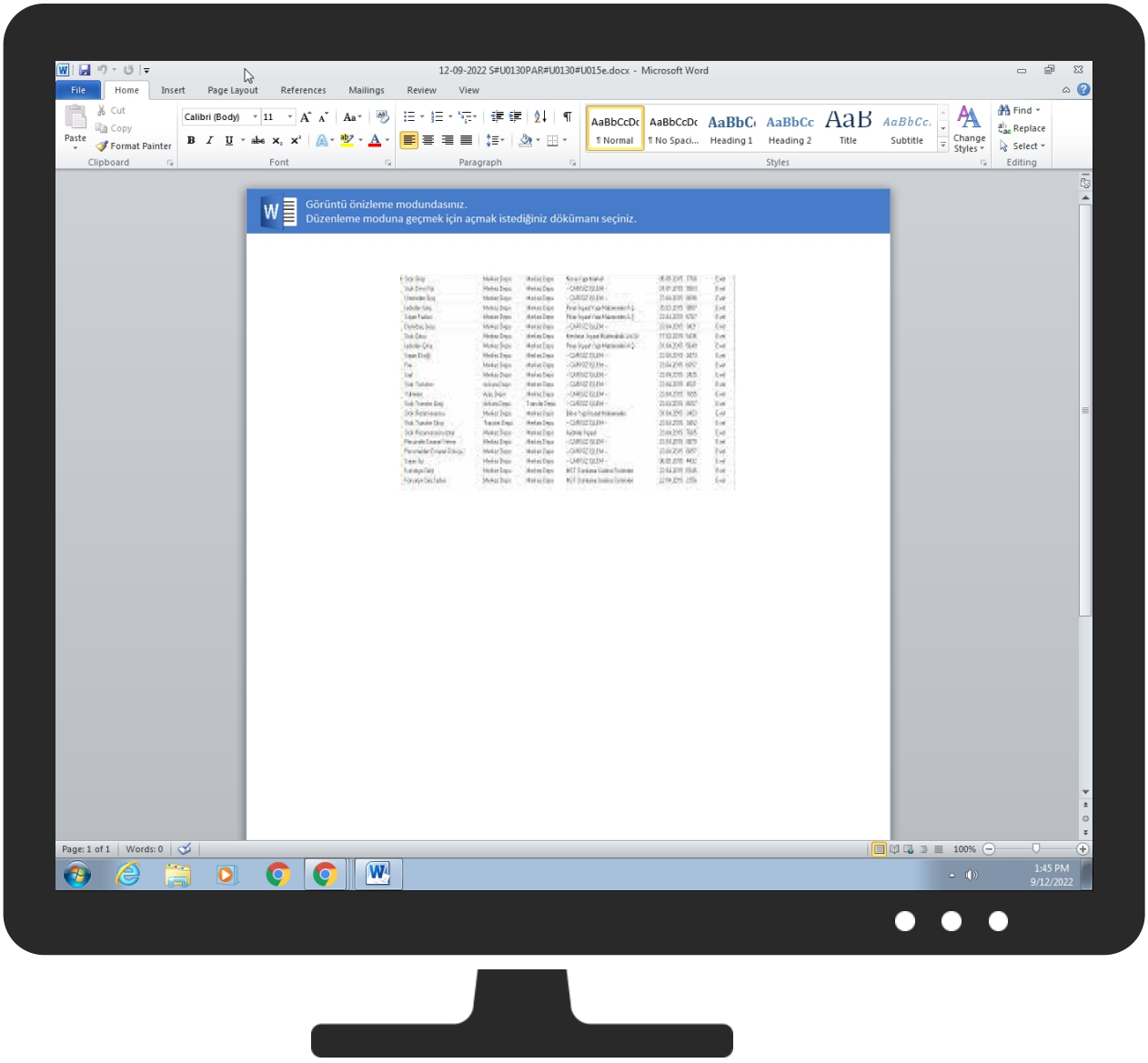


Screenshots

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
12-09-2022 S#U0130PAR#U0130#U015e.docx.doc	27%	ReversingLabs	ByteCode-JAVA.Downloader.BanLoad	
12-09-2022 S#U0130PAR#U0130#U015e.docx.doc	17%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://java.sun.com/xml/dom/properties/(	0%	URL Reputation	safe	
http://java.sun.com/xml/dom/properties/(	0%	URL Reputation	safe	
http://java.sun.com/xml/schema/features/	0%	URL Reputation	safe	
http://java.sun.com/xml/dom/properties/	0%	URL Reputation	safe	
http://javax.xml.XMLConstants/feature/secure-processing	0%	URL Reputation	safe	
http://javax.xml.XMLConstants/property/accessExternalSchema	0%	URL Reputation	safe	
http://java.sun.com/xml/schema/features/report-ignored-element-content-whitespace0	0%	URL Reputation	safe	
http://java.sun.com/xml/stream/properties/report-cdata-event	0%	URL Reputation	safe	
http://bugreport.sun.com/bugreport/	0%	URL Reputation	safe	
http://bugreport.sun.com/bugreport/	0%	URL Reputation	safe	
http://java.sun.com/dtd/properties.dtd	0%	URL Reputation	safe	
http://javax.xml.XMLConstants/property/accessExternalDTD;	0%	URL Reputation	safe	
http://java.sun.com/xml/dom/properties/ancestor-check	0%	URL Reputation	safe	
http://java.sun.com/xml/stream/properties/	0%	URL Reputation	safe	
http://javax.xml.XMLConstants/property/accessExternalSchemas3p	0%	Avira URL Cloud	safe	
http://java.sun.com/xml/stream/properties/ignore-external-dtdV	0%	Avira URL Cloud	safe	
http://javax.xml.XMLConstants/property/accessExternalDTDs	0%	Avira URL Cloud	safe	
http://java.sun.com/xml/schema/features/report-ignored-element-content-whitespace;	0%	Avira URL Cloud	safe	
http://java.sun.com/dtd/properties.dtd3	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://javax.xml.XMLConstants/property/accessExternalSchemas3p	javaw.exe, 00000003.00000002.1047788279.00000000D7534000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://apache.org/xml/features/dom/create-entity-ref-nodes	javaw.exe, 00000003.00000003.967137901.0 000000058DE3000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.961343704.0000000058DB2000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.963476262.000000 0058DD5000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1006841983.00000000 58DEB000.00000004.00000020.00020000.0000 0000.sdmp, javaw.exe, 00000003.00000003. 962280568.0000000058DCE000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.965067072.0000000058DD C000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp, javaw.exe, 0000000A.0000 0003.989124167.00000000591DB000.00000004 .00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1064044169.0000000059262000 .00000004.00000020.00020000.00000000.sdmp	false		high
http://java.sun.com/xml/dom/properties/(	javaw.exe, 00000003.00000003.963573067.0 00000005900B000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.967436542.000000005901A000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.962440979.0000000058FFB00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960930096.0000000 058FC6000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 0000000A.00000003 .987388038.0000000059ABA000.00000004.000 00020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://apache.org/xml/features/validation/dynamic	javaw.exe, 00000003.00000002.1049410615. 00000000D7693000.00000004.00000800.00020 000.00000000.sdmp, javaw.exe, 0000000A.0 0000002.1116728587.00000000D76EE000.0000 0004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/validation/schema/augment-psvi	javaw.exe, 0000000A.00000003.987388038.0 000000059ABA000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 0000000A.00 000002.1116728587.00000000D76EE000.00000 004.00000800.00020000.00000000.sdmp	false		high
http://java.sun.com/xml/schema/features/	javaw.exe, 00000003.00000003.963573067.0 00000005900B000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.967436542.000000005901A000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.962440979.0000000058FFB00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960930096.0000000 058FC6000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 00000003.00000002 .1049410615.00000000D7693000.00000004.00 000800.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059 ABA000.00000004.00000020.00020000.000000 00.sdmp, javaw.exe, 0000000A.00000002.11 16728587.00000000D76EE000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://xml.org/sax/features/tream$PutFie	javaw.exe, 00000003.00000003.963573067.0 00000005900B000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.967436542.000000005901A000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.962440979.0000000058FFB00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960930096.0000000 058FC6000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 0000000A.00000003 .987388038.0000000059ABA000.00000004.000 00020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://apache.org/xml/properties/internal/validator/dtd	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.000000 00599CA000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.000000005 9A0A000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 00000003.00000002.1 008031716.0000000059A19000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059AB A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://apache.org/xml/properties/input-buffer-size	javaw.exe, 00000003.00000002.1047788279. 00000000D7534000.00000004.00000800.00020 000.00000000.sdmp, javaw.exe, 00000003.0 0000002.1049410615.00000000D7693000.0000 0004.00000800.00020000.00000000.sdmp, ja vaw.exe, 0000000A.00000002.1116728587.00 000000D76EE000.00000004.00000800.0002000 0.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/datatype-validator-factory	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1049410615.000000 00D7693000.00000004.00000800.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 3.964787205.0000000059A0A000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008031716.000000005 9A19000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 0000000A.00000003.9 87388038.0000000059ABA000.00000004.00000 020.00020000.00000000.sdmp, javaw.exe, 0 000000A.00000002.1116728587.00000000D76E E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/validator/schema	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.000000 00599CA000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.000000005 9A0A000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 00000003.00000002.1 008031716.0000000059A19000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059AB A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://apache.org/xml/features/internal/parser-settingss8q	javaw.exe, 00000003.00000002.1047788279. 00000000D7534000.00000004.00000800.00020 000.00000000.sdmp	false		high
http://apache.org/xml/features/internal/tolerate-duplicatesO	javaw.exe, 0000000A.00000003.987388038.0 000000059ABA000.00000004.00000020.000200 00.00000000.sdmp	false		high
http://apache.org/xml/features/validate-annotations	javaw.exe, 0000000A.00000003.987388038.0 000000059ABA000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 0000000A.00 000002.1116728587.00000000D76EE000.00000 004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/standard-uri-conformantK	javaw.exe, 00000003.00000002.1047788279. 00000000D7534000.00000004.00000800.00020 000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://apache.org/xml/properties/schema/external-schemaLocation(	javaw.exe, 0000000A.00000003.987388038.0 000000059ABA000.00000004.00000020.000200 00.00000000.sdmp	false		high
http://java.oracle.com/sha	javaw.exe, 0000000A.00000002.1067403383. 00000000D5580000.00000004.00000800.00020 000.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/namespace-contextV	javaw.exe, 0000000A.00000003.987388038.0 000000059ABA000.00000004.00000020.000200 00.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/entity-manager	javaw.exe, 00000003.00000002.1047788279. 00000000D7534000.00000004.00000800.00020 000.00000000.sdmp, javaw.exe, 00000003.0 0000002.1049410615.00000000D7693000.0000 0004.00000800.00020000.00000000.sdmp, ja vaw.exe, 0000000A.00000002.1116728587.00 000000D76EE000.00000004.00000800.0002000 0.00000000.sdmp	false		high
http://apache.org/xml/features/dom/create-entity-ref-nodes?	javaw.exe, 00000003.00000003.967137901.0 000000058DE3000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.961343704.0000000058DB2000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.963476262.0000000058DD500 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1006841983.000000 0058DEB000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 3.962280568.0000000058DCE000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.965067072.0000000058 DDC000.00000004.00000020.00020000.000000 00.sdmp, javaw.exe, 0000000A.00000003.98 9124167.00000000591DB000.00000004.000000 20.00020000.00000000.sdmp, javaw.exe, 00 00000A.00000002.1064044169.0000000059262 000.00000004.00000020.00020000.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/dtd-processor	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1049410615.000000 00D7693000.00000004.00000800.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 3.964787205.0000000059A0A000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008031716.000000005 9A19000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 0000000A.00000003.9 87388038.0000000059ABA000.00000004.00000 020.00020000.00000000.sdmp, javaw.exe, 0 000000A.00000002.1116728587.00000000D76E E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/namespace-growth	javaw.exe, 0000000A.00000003.987388038.0 000000059ABA000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 0000000A.00 000002.1116728587.00000000D76EE000.00000 004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/properties/dom/document-class-name$	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000 059A0A000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 00000003.00000002 .1008031716.0000000059A19000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059 ABA000.00000004.00000020.00020000.000000 00.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://apache.org/xml/properties/internal/symbol-tableQ	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000 059A0A000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 00000003.00000002 .1008031716.0000000059A19000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059 ABA000.00000004.00000020.00020000.000000 00.sdmp	false		high
http://apache.org/xml/features/internal/parser-settings	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1049410615.000000 00D7693000.00000004.00000800.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 3.964787205.0000000059A0A000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008031716.000000005 9A19000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 0000000A.00000003.9 87388038.0000000059ABA000.00000004.00000 020.00020000.00000000.sdmp, javaw.exe, 0 000000A.00000002.1116728587.00000000D76E E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/dom/include-ignorable-whitespace	javaw.exe, 00000003.00000003.967137901.0 000000058DE3000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.961343704.0000000058DB2000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.963476262.000000 0058DD5000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1006841983.00000000 58DEB000.00000004.00000020.00020000.0000 0000.sdmp, javaw.exe, 00000003.00000003. 962280568.0000000058DCE000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.965067072.0000000058DD C000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp, javaw.exe, 0000000A.0000 0003.989124167.00000000591DB000.00000004 .00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1064044169.0000000059262000 .00000004.00000020.00020000.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/document-scanner7	javaw.exe, 0000000A.00000003.987388038.0 000000059ABA000.00000004.00000020.000200 00.00000000.sdmp	false		high
http://xml.org/sax/features/allow-dtd-events-after-endDTD=	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000 059A0A000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 00000003.00000002 .1008031716.0000000059A19000.00000004.00 000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://apache.org/xml/features/create-cdata-nodes	javaw.exe, 00000003.00000003.967137901.0 000000058DE3000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.961343704.0000000058DB2000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.963476262.000000 0058DD5000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1006841983.00000000 58DEB000.00000004.00000020.00020000.0000 0000.sdmp, javaw.exe, 00000003.00000003. 962280568.0000000058DCE000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.965067072.0000000058DD C000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp, javaw.exe, 0000000A.0000 0003.989124167.00000000591DB000.00000004 .00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1064044169.0000000059262000 .00000004.00000020.00020000.00000000.sdmp	false		high
http://java.sun.com/xml/dom/properties/	javaw.exe, 00000003.00000002.1048181873. 00000000D7576000.00000004.00000800.00020 000.00000000.sdmp, javaw.exe, 00000003.0 0000003.963573067.000000005900B000.00000 004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.967436542.000000005901A0 00.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.962440979.000000 0058FFB000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 3.960930096.0000000058FC6000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1049410615.00000000D 7693000.00000004.00000800.00020000.00000 000.sdmp, javaw.exe, 0000000A.00000003.9 87388038.0000000059ABA000.00000004.00000 020.00020000.00000000.sdmp, javaw.exe, 0 000000A.00000002.1116728587.00000000D76E E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://apache.org/xml/properties/internal/document-scannerk	javaw.exe, 00000003.00000002.1047788279. 00000000D7534000.00000004.00000800.00020 000.00000000.sdmp	false		high
http://javax.xml.XMLConstants/property/accessExternalDTDs	javaw.exe, 00000003.00000002.1047788279. 00000000D7534000.00000004.00000800.00020 000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://apache.org/xml/properties/internal/stax-entity-resolver	javaw.exe, 00000003.00000002.1047788279. 00000000D7534000.00000004.00000800.00020 000.00000000.sdmp, javaw.exe, 00000003.0 0000002.1049410615.00000000D7693000.0000 0004.00000800.00020000.00000000.sdmp, ja vaw.exe, 0000000A.00000002.1116728587.00 000000D76EE000.00000004.00000800.0002000 0.00000000.sdmp	false		high
http://apache.org/xml/features/scanner/notify-char-refs3	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000 059A0A000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 00000003.00000002 .1008031716.0000000059A19000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059 ABA000.00000004.00000020.00020000.000000 00.sdmp	false		high
http://apache.org/xml/features/3	javaw.exe, 0000000A.00000003.987388038.0 000000059ABA000.00000004.00000020.000200 00.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://apache.org/xml/features/xinclude/fixup-base-uris6	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000 059A0A000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 00000003.00000002 .1008031716.0000000059A19000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059 ABA000.00000004.00000020.00020000.000000 00.sdmp	false		high
http://javax.xml.XMLConstants/feature/secure-processing	javaw.exe, 00000003.00000003.967137901.0 000000058DE3000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.961343704.0000000058DB2000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.963476262.000000 0058DD5000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1006841983.00000000 58DEB000.00000004.00000020.00020000.0000 0000.sdmp, javaw.exe, 00000003.00000003. 962280568.0000000058DCE000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.965067072.0000000058DD C000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp, javaw.exe, 0000000A.0000 0003.989124167.00000000591DB000.00000004 .00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1064044169.0000000059262000 .00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://apache.org/xml/features/xinclude/fixup-base-uris	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.000000 00599CA000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.000000005 9A0A000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 00000003.00000002.1 008031716.0000000059A19000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059AB A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://apache.org/xml/properties/internal/grammar-pool6	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000 059A0A000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 00000003.00000002 .1008031716.0000000059A19000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059 ABA000.00000004.00000020.00020000.000000 00.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://apache.org/xml/properties/schema/external-noNamespaceSchemaLocation	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1049410615.000000 00D7693000.00000004.00000800.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 3.964787205.0000000059A0A000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008031716.000000005 9A19000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 0000000A.00000003.9 87388038.0000000059ABA000.00000004.00000 020.00020000.00000000.sdmp, javaw.exe, 0 000000A.00000002.1116728587.00000000D76E E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/error-reporter	javaw.exe, 00000003.00000002.1047788279. 00000000D7534000.00000004.00000800.00020 000.00000000.sdmp, javaw.exe, 00000003.0 0000002.1049410615.00000000D7693000.0000 0004.00000800.00020000.00000000.sdmp, ja vaw.exe, 0000000A.00000002.1116728587.00 000000D76EE000.00000004.00000800.0002000 0.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/namespace-context	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1049410615.000000 00D7693000.00000004.00000800.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 3.964787205.0000000059A0A000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008031716.000000005 9A19000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 0000000A.00000002.1 116728587.00000000D76EE000.00000004.0000 0800.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/warn-on-duplicate-entitydef	javaw.exe, 0000000A.00000003.987388038.0 000000059ABA000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 0000000A.00 000002.1116728587.00000000D76EE000.00000 004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/;	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000 059A0A000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 00000003.00000002 .1008031716.0000000059A19000.00000004.00 000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ipinfo.io/	javaw.exe, 00000003.00000003.962713926.0 000000059BA0000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964855770.0000000059A6F000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.962091806.0000000059B7900 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1048874613.000000 00D763A000.00000004.00000800.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 3.966236710.0000000059A76000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008117482.000000005 9A95000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 00000003.00000002.1 046320748.00000000D745E000.00000004.0000 0800.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1046522557.00000000D74 7C000.00000004.00000800.00020000.0000000 0.sdmp, javaw.exe, 00000003.00000003.966 642599.0000000059A95000.00000004.0000002 0.00020000.00000000.sdmp, javaw.exe, 000 00003.00000003.958316594.0000000059A6F00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.956399008.0000000 059B48000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 0000000A.00000003 .1009441017.0000000059731000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1115594736.00000000D 7648000.00000004.00000800.00020000.00000 000.sdmp, javaw.exe, 0000000A.00000003.1 006410957.000000005984C000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.1002287620.00000000596 C2000.00000004.00000020.00020000.0000000 0.sdmp, javaw.exe, 0000000A.00000002.110 7668636.00000000D7424000.00000004.000008 00.00020000.00000000.sdmp, javaw.exe, 00 00000A.00000002.1064752540.0000000059731 000.00000004.00000020.00020000.00000000.sdmp	false		high
http://java.sun.com/dtd/properties.dtd3	javaw.exe, 00000003.00000002.1047788279. 00000000D7534000.00000004.00000800.00020 000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://apache.org/xml/features/scanner/notify-char-refsC	javaw.exe, 00000003.00000002.1047788279. 00000000D7534000.00000004.00000800.00020 000.00000000.sdmp	false		high
http://javax.xml.XMLConstants/property/accessExternalSchema	javaw.exe, 0000000A.00000002.1064044169. 0000000059262000.00000004.00000020.00020 000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://java.sun.com/xml/schema/features/report-ignored-element-content-whitespace;	javaw.exe, 00000003.00000002.1047788279. 00000000D7534000.00000004.00000800.00020 000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://xml.org/sax/properties/(	javaw.exe, 0000000A.00000003.987388038.0 000000059ABA000.00000004.00000020.000200 00.00000000.sdmp	false		high
http://apache.org/xml/features/include-comments	javaw.exe, 00000003.00000003.967137901.0 000000058DE3000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.961343704.0000000058DB2000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.963476262.0000000058DD500 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1049410615.000000 00D7693000.00000004.00000800.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1006841983.0000000058DEB000.00000004.0 0000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.962280568.000000005 8DCE000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 00000003.00000003.9 65067072.0000000058DDC000.00000004.00000 020.00020000.00000000.sdmp, javaw.exe, 0 000000A.00000002.1116728587.00000000D76E E000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.989124167.0000 0000591DB000.00000004.00000020.00020000. 00000000.sdmp, javaw.exe, 0000000A.00000 002.1064044169.0000000059262000.00000004 .00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://apache.org/xml/features/scanner/notify-char-refs	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1049410615.000000 00D7693000.00000004.00000800.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 3.964787205.0000000059A0A000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008031716.000000005 9A19000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 0000000A.00000003.9 87388038.0000000059ABA000.00000004.00000 020.00020000.00000000.sdmp, javaw.exe, 0 000000A.00000002.1116728587.00000000D76E E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/internal/tolerate-duplicatesY	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000 059A0A000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 00000003.00000002 .1008031716.0000000059A19000.00000004.00 000020.00020000.00000000.sdmp	false		high
http://apache.org/xml/properties/dom/current-element-node9	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000 059A0A000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 00000003.00000002 .1008031716.0000000059A19000.00000004.00 000020.00020000.00000000.sdmp	false		high
http://java.sun.com/xml/schema/features/report-ignored-element-content-whitespace0	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000 059A0A000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 00000003.00000002 .1008031716.0000000059A19000.00000004.00 000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://java.sun.com/xml/stream/properties/report-cdata-event	javaw.exe, 00000003.00000002.1007607362. 000000005912A000.00000004.00000020.00020 000.00000000.sdmp, javaw.exe, 00000003.0 0000003.961135410.0000000059112000.00000 004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.967577855.000000005911F0 00.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.1018446449.00000 000591B3000.00000004.00000020.00020000.0 0000000.sdmp, javaw.exe, 0000000A.000000 03.1014550524.00000000591AB000.00000004. 00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.1008158290.0000000 059149000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 0000000A.00000003 .991312019.00000000590C9000.00000004.000 00020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1063932993.0000000059 1BA000.00000004.00000020.00020000.000000 00.sdmp	false	• URL Reputation: safe	unknown
http://apache.org/xml/features/nonvalidating/load-external-dtd:	javaw.exe, 0000000A.00000003.987388038.0 000000059ABA000.00000004.00000020.000200 00.00000000.sdmp	false		high
http://apache.org/xml/features/validation/schema/normalized-valueB	javaw.exe, 0000000A.00000003.987388038.0 000000059ABA000.00000004.00000020.000200 00.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://apache.org/xml/features/continue-after-fatal-error	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.000000 00599CA000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.000000005 9A0A000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 00000003.00000002.1 008031716.0000000059A19000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059AB A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://apache.org/xml/features/standard-uri-conformant	javaw.exe, 00000003.00000002.1049410615. 00000000D7693000.00000004.00000800.00020 000.00000000.sdmp, javaw.exe, 0000000A.0 0000002.1116728587.00000000D76EE000.0000 0004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/document-scanner	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1049410615.000000 00D7693000.00000004.00000800.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 3.964787205.0000000059A0A000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008031716.000000005 9A19000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 0000000A.00000003.9 87388038.0000000059ABA000.00000004.00000 020.00020000.00000000.sdmp, javaw.exe, 0 000000A.00000002.1116728587.00000000D76E E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/validation/schema/dv-factory7	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000 059A0A000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 00000003.00000002 .1008031716.0000000059A19000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059 ABA000.00000004.00000020.00020000.000000 00.sdmp	false		high
http://xml.org/sax/features/use-entity-resolver2	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.000000 00599CA000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.000000005 9A0A000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 00000003.00000002.1 008031716.0000000059A19000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059AB A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://bugreport.sun.com/bugreport/	javaw.exe, 00000003.00000002.1048681741.00000000D7615000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1010127537.00000000D5580000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1067403383.00000000D5580000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://apache.org/xml/properties/internal/entity-resolver	javaw.exe, 00000003.00000003.966664801.0000000059A11000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964657582.00000000599EA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D7534000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1049410615.00000000D7693000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000059A0A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008031716.0000000059A19000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.00000000D76EE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://java.oracle.com/	javaw.exe, 00000003.00000002.1048681741.00000000D7615000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1010127537.00000000D5580000.00000004.00000800.00020000.00000000.sdmp	false		high
http://xml.org/sax/properties/C	javaw.exe, 00000003.00000002.1047788279.00000000D7534000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/	javaw.exe, 00000003.00000003.966664801.0000000059A11000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964657582.00000000599EA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D7534000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1049410615.00000000D7693000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000059A0A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008031716.0000000059A19000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059ABA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.00000000D76EE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/generate-synthetic-annotations	javaw.exe, 00000003.00000003.966664801.0000000059A11000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964657582.00000000599EA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D7534000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1049410615.00000000D7693000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000059A0A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008031716.0000000059A19000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059ABA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.00000000D76EE000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://apache.org/xml/features/standard-uri-conformanter2	javaw.exe, 00000003.00000003.963573067.000000005900B000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.967436542.000000005901A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.962440979.0000000058FFB000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960930096.0000000058FC6000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.1009441017.0000000059731000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.1002287620.0000000596C2000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1064752540.0000000059731000.00000004.00000020.00020000.00000000.sdmp	false		high
http://java.sun.com/dtd/properties.dtd	javaw.exe, 00000003.00000002.1049410615.00000000D7693000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1006841983.0000000058DEB000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1048641447.000000D7608000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.962280568.0000000058DCE000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.965067072.0000000058DDC000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1109407547.0000000D755D000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.00000000D76EE000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.989124167.00000000591DB000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1107668636.00000000D7424000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1109311234.00000000D7549000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1064044169.0000000059262000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://xml.org/sax/features/allow-dtd-events-after-endDTD	javaw.exe, 00000003.00000003.966664801.000000059A11000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964657582.00000000599EA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D7534000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1049410615.00000000D7693000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000059A0A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008031716.0000000059A19000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059ABA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.00000000D76EE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/validation/balance-syntax-trees	javaw.exe, 00000003.00000002.1049410615.00000000D7693000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.00000000D76EE000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://java.sun.com/xml/stream/properties/ignore-external-dtdV	javaw.exe, 00000003.00000003.963573067.000000005900B000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.967436542.000000005901A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.962440979.0000000058FFB000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960930096.0000000058FC6000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.1009441017.0000000059731000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.1002287620.00000005596C2000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1064752540.0000000059731000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://apache.org/xml/features/include-comments0	javaw.exe, 0000000A.00000003.989124167.000000000591DB000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1064044169.0000000059262000.00000004.00000020.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/internal/validation/schema/use-grammar-pool-only	javaw.exe, 00000003.00000003.966664801.000000059A11000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964657582.00000000599EA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D7534000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1049410615.00000000D7693000.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000059A0A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008031716.0000000059A19000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059ABA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.00000000D76EE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/properties/schema/external-noNamespaceSchemaLocation;	javaw.exe, 00000003.00000002.1047788279.00000000D7534000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/validation/balance-syntax-treesK	javaw.exe, 00000003.00000002.1047788279.00000000D7534000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/namespace-binder	javaw.exe, 0000000A.00000003.987388038.0000000059ABA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.00000000D76EE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://javax.xml.XMLConstants/property/accessExternalDTD;	javaw.exe, 00000003.00000003.967137901.000000058DE3000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.961343704.0000000058DB2000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.963476262.0000000058DD5000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1006841983.0000000058DEB000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.962280568.0000000058DCE000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.965067072.0000000058DDC000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.989124167.00000000591DB000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1064044169.0000000059262000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ipinfo.io/ipX	javaw.exe, 00000003.00000003.958316594.000000059A6F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/validation/schema/augment-psviK	javaw.exe, 00000003.00000002.1047788279.00000000D7534000.00000004.00000800.00020000.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/namespace-contextk5p	javaw.exe, 00000003.00000002.1047788279.00000000D7534000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://xml.org/sax/features/validation	javaw.exe, 00000003.00000003.967137901.0 000000058DE3000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.961343704.0000000058DB2000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.963476262.000000 0058DD5000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1006841983.00000000 58DEB000.00000004.00000020.00020000.0000 0000.sdmp, javaw.exe, 00000003.00000003. 962280568.0000000058DCE000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.965067072.0000000058DD C000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp, javaw.exe, 0000000A.0000 0003.989124167.00000000591DB000.00000004 .00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1064044169.0000000059262000 .00000004.00000020.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/scanner/notify-builtin-refs7	javaw.exe, 0000000A.00000003.987388038.0 000000059ABA000.00000004.00000020.000200 00.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/namespace-context:	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000 059A0A000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 00000003.00000002 .1008031716.0000000059A19000.00000004.00 000020.00020000.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/xinclude-handler	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.000000 00599CA000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.000000005 9A0A000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 00000003.00000002.1 008031716.0000000059A19000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059AB A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://apache.org/xml/properties/security-manager	javaw.exe, 00000003.00000003.967137901.0 000000058DE3000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.961343704.0000000058DB2000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.963476262.000000 0058DD5000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1006841983.00000000 58DEB000.00000004.00000020.00020000.0000 0000.sdmp, javaw.exe, 00000003.00000003. 962280568.0000000058DCE000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.965067072.0000000058DD C000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp, javaw.exe, 0000000A.0000 0003.989124167.00000000591DB000.00000004 .00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1064044169.0000000059262000 .00000004.00000020.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/validation/schema/augment-psvic	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.0000000 059A0A000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 00000003.00000002 .1008031716.0000000059A19000.00000004.00 000020.00020000.00000000.sdmp	false		high
http://java.sun.com/xml/dom/properties/ancestor-check	javaw.exe, 00000003.00000003.966821739.0 000000059CA4000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000002.1048041021.00000000D7561000.00000 004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.967357824.0000000059CA40 00.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008328551.00000 00059CA4000.00000004.00000020.00020000.0 0000000.sdmp, javaw.exe, 00000003.000000 02.1049410615.00000000D7693000.00000004. 00000800.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1109407547.0000000 0D755D000.00000004.00000800.00020000.000 00000.sdmp, javaw.exe, 0000000A.00000002 .1065071207.0000000059885000.00000004.00 000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.1006601184.000000005 986D000.00000004.00000020.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://apache.org/xml/features/namespace-growthK	javaw.exe, 00000003.00000002.1047788279. 00000000D7534000.00000004.00000800.00020 000.00000000.sdmp	false		high
http://java.sun.com/xml/stream/properties/	javaw.exe, 00000003.00000002.1048181873. 00000000D7576000.00000004.00000800.00020 000.00000000.sdmp, javaw.exe, 00000003.0 0000002.1049410615.00000000D7693000.0000 0004.00000800.00020000.00000000.sdmp, ja vaw.exe, 0000000A.00000002.1116728587.00 000000D76EE000.00000004.00000800.0002000 0.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.oracle.com/feature/use-service-mechanismjectI	javaw.exe, 00000003.00000003.963573067.0 00000005900B000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.967436542.000000005901A000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.962440979.0000000058FFB00 0.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960930096.0000000 058FC6000.00000004.00000020.00020000.000 00000.sdmp, javaw.exe, 0000000A.00000003 .987388038.0000000059ABA000.00000004.000 00020.00020000.00000000.sdmp	false		high
http://apache.org/xml/features/validation/schema	javaw.exe, 0000000A.00000002.1064044169. 0000000059262000.00000004.00000020.00020 000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://apache.org/xml/properties/internal/dtd-scanner	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.000000 00599CA000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.000000005 9A0A000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 00000003.00000002.1 008031716.0000000059A19000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059AB A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://apache.org/xml/features/validation/warn-on-undeclared-elemdefs	javaw.exe, 00000003.00000002.1047788279. 00000000D7534000.00000004.00000800.00020 000.00000000.sdmp	false		high
http://apache.org/xml/properties/schema/external-schemaLocation	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.000000 00599CA000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.000000005 9A0A000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 00000003.00000002.1 008031716.0000000059A19000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059AB A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://xml.org/sax/features/	javaw.exe, 00000003.00000002.1048181873. 00000000D7576000.00000004.00000800.00020 000.00000000.sdmp, javaw.exe, 00000003.0 0000002.1049410615.00000000D7693000.0000 0004.00000800.00020000.00000000.sdmp, ja vaw.exe, 0000000A.00000002.1116728587.00 000000D76EE000.00000004.00000800.0002000 0.00000000.sdmp	false		high
http://apache.org/xml/properties/internal/error-handler	javaw.exe, 00000003.00000003.966664801.0 000000059A11000.00000004.00000020.000200 00.00000000.sdmp, javaw.exe, 00000003.00 000003.964657582.00000000599EA000.000000 04.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1047788279.00000000D75340 00.00000004.00000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.000000 00599CA000.00000004.00000020.00020000.00 000000.sdmp, javaw.exe, 00000003.0000000 2.1049410615.00000000D7693000.00000004.0 0000800.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.000000005 9A0A000.00000004.00000020.00020000.00000 000.sdmp, javaw.exe, 00000003.00000002.1 008031716.0000000059A19000.00000004.0000 0020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000003.987388038.0000000059AB A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 0000000A.00000002.1116728587.000 00000D76EE000.00000004.00000800.00020000 .00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://apache.org/xml/features/validation/schema-full-checkingP	javaw.exe, 00000003.00000003.966664801.000000059A11000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964657582.00000000599EA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.960812434.00000000599CA000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000003.964787205.00000000059A0A000.00000004.00000020.00020000.00000000.sdmp, javaw.exe, 00000003.00000002.1008031716.0000000059A19000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	701320
Start date and time:	2022-09-12 13:44:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	12-09-2022 S#U0130PAR#U0130#U015e.docx.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.troj.expl.evad.winDOC@21/13@0/0
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 • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe
- Execution Graph export aborted for target javaw.exe, PID 1316 because it is empty
- Execution Graph export aborted for target javaw.exe, PID 1952 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile 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
13:45:42	API Interceptor	158x Sleep call for process: WMIC.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\Oracle\Java\.oracle_jre_usage\17dfc292991c7c05.timestamp

Process:	C:\Program Files\Java\jre1.8.0_121\bin\javaw.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	51
Entropy (8bit):	4.666852547556904
Encrypted:	false
SSDEEP:	3:oFjQvN1SkQVy:oy1rAy
MD5:	B346612A2A15D30EF8E4899093BD9C1D
SHA1:	8ECA61C2A0C83684C036F5D22A002C129DF3AD2A
SHA-256:	C24A7ABE525ABD5426D3782990E37ABBCF6F28AB41E64F3132A1162B8019488D
SHA-512:	0ADEEEC8F52D912698DCA98D127381922959C5D02B706523C18C88C4E04668BB1A2601FC55CE427A13C29BF0BBFEAE6C07BB66E6A40FDE9C8420631CA7169E21
Malicious:	false
Preview:	C:\Program Files\Java\jre1.8.0_121..1663015551990..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\37821B9D.emf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	5464
Entropy (8bit):	0.8660964834720057

Encrypted:	false
SSDEEP:	12:YaFmecr6gSbfMqH18JM8XqVlwcb1KCu6Tj/4KCJfBoWLBzbmYXi6UgoemYJ:Ya0r6gSbfm/qVuCREkWLB+B6Ug4y
MD5:	C2D8244DD18F565035212FC52D3F4E75
SHA1:	8C85DDF7655242B178D77F7BEB81D2E3BEB9F35B
SHA-256:	89CB85E37E9623CD2B091B539C6E1280AA39E21CF7B6B0A54F5FDA180A197B98
SHA-512:	4EBA9EC61253B67231E854906AEA3DB0D37276ED9A7034661781612C5D69A41B8917ABEC40FACD9A2C6A4A3CD2220019A360B9AF6F01F52C118658C52D81324C
Malicious:	false
Preview:	....l...#.......B... ..... EMF....X.....V.....i.....M...$...#.....B... ...#..... ... .?.....?.....l...0..... ... ...(... ..".. .....M.....#.....B... ...#..... ... ...F.f.....?.....?.....l.. .4..... ... ...(... ... .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5AF0F4FA.png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 706 x 366, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68893
Entropy (8bit):	7.903401375792054
Encrypted:	false
SSDEEP:	1536:BsvJG1S1KOhGCAZmweGEjZv9mX+DZL8mI2dEN2vT4q+b:OvJM0AZUr1v9BZQOsq+b
MD5:	94C3E4696F04CB7960042417CF39FE07
SHA1:	EC45840F87B3AC5812F9CE765CD398AEEB2A659C
SHA-256:	A1566D12B7BEE123511040635AE34D71E23AE1F73706347EB5926A61AB72BDB7
SHA-512:	8FBDE178BA6DFD021B9E43CA6ADC205F6AB8939E6FE93807C20E9FA8D808DFED1E13D4EE485A3B13932452070FABA749E83EF7795A70F1A75B26081C86C399DA
Malicious:	false
Preview:	.PNG.....IHDR.....n.....$~.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.....%\|..K?.k...f..eU/U.....RR.D..8...N.8.$@. .. @..<..D &L...o...[..#B....e..?...a....q...v... ;..~.f.....3w8s+xe.Bpbz4."8>v...M./.N.Go..^...^.q3xi.w.,.]...:.....D...T.B.~.....r.....e..0.]M8:.....uF.L,('...NO..^.<.....t-x... .6..s..W.....t.V/o.^...t.t}....+A....V.....&n...52..z. ....>.:..y}&x.....sg.....#Amv/.w/.N..z.....N...P{....qk...qld..m..}^.0.....c....zqix...`.....C.....>6..w.5....^;.....`...t....^.mh\nN..u..E.:^\\.....q.>...0>:..p.J..p..e.igV..t..w.....>.....Pk .Z..Z...K=..pl.r...^O....H.....[S.K.....S..S....9}..gN..N]...5.;..L.^..<z$..>.v...^.e..._..~.....t.....[.....9..j...+=.2.....#..7'....{;.NO].....,H...q..^....8W..0o.{.....;....\|..x...r..#...w.S7o. ..=.t...=.6.^...c...O_8.....^..tC...7z?$f..g....?.t..^4.^...:.....O....,..q.f..g.:..{.2...W/.G....9....:r.m..#=.<K..s}...n..<q.dp

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8C420CB3.PNG

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 1037 x 72, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	8976
Entropy (8bit):	7.80633939156706
Encrypted:	false
SSDEEP:	192:r/UrdFouQWn/Mjnh2LqFNB7pf/VVC8dOx9MRMbQMAIimhM6we4RxCofEq:jUrQuQJELc1VI8sx6MbQMAIVGRxdcq
MD5:	25902859A8786C02C68F6AA66C151C7C
SHA1:	8829DDF4BC5CB5AB8A4C510CAD67B27FE3EE2BE9
SHA-256:	67BA24DD3354C3E058B032FBAF799D9F0D11FD35FA9B80A9DEDAA3ABFFE32893
SHA-512:	895801C640F737FF5F1DB6A14A91AC2B91A3CC2CA5070C9B97D2F3C4EE2097E2ADCA219496E8EE120CCEA58B88BE435FA256AA1D699D7D413A3F1C5ACE2A1F7E
Malicious:	false
Preview:	.PNG.....IHDR.....H.....!....sRGB.....gAMA.....a.....pHYs.....+....".IDATx^.....y.}...}..!.....:..;....EH1.$.;N..2!.p.S.H..P.J..Bd....?.qB.....H...e..QH\9.OXHB>.t .t.{... ggg.n{gwN{..w....<.w4.7_w'.....H.....(.....J.....B..J.....0.....4J.B~.F..h..(...V..Q"I.T....)..?fJ.....4(..b90<p.....7...oR2..t&GM.....iJ ..m\....4.....V.h.~..8y. ....L7Q:;..3...@...M..x.8.QF.....\i..AA.....n.{....y...%.'3...\.\|.~.y.J7.].F..p.}I2..V.H@9.....ji...F.O..o.r...O.h.....R9JO.C.3.....D3 {.V..*.W ....`.....P=1*.....=....:.....z....}....w...)J..(.4E.g..{...y...Dd.6b@...,.<.L..+.....$...X$.7~E...P"..dJ9...xJ....'.4.O%).Pq.'.W....qj#..O..&...j.2*p....\|..3.J^....e.E.....`... .@.^.N..A..0...Q.$.&.Ti.}V..Q... .S.(g4.v8..00.....!.w.o...\@MMM*.....{GL.....|.6<....C.Xz..<.u....p.....2...W.&T.f...$M9..X=...J.....z.|D.....`R...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{D598F5A9-41E1-44C7-8D38-8B82E1D2FAA1}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	337464
Entropy (8bit):	7.97260257732735
Encrypted:	false
SSDEEP:	6144:PHtmJnbEwVak+5BoY6/KcWbokztmJnbEwVak+5BoY6/KcWbon:/MJnbEwYkUoYRpMSMJnbEwYkUoYRpMn
MD5:	799293EED30AE65B8A03E2BF2C14EFB2
SHA1:	643FA005DC68F0345A6E1EDD37D0745C0855A3CC

SHA-256:	D0CE7CA37043D297A7D9082FAD159D71E1E3732B38D41C3CBD9CA9C855AB93EE
SHA-512:	8A13024D23F3D0F10061956AC08D2E8D8EF4C254EB89825BE7417039844903FA46AB79F40006A48F83DEDE3D81B9951750BA6F01E70663C24F09C832D35A17A8
Malicious:	false
Preview:	.....>.....M...N...O..... .....J... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A... B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v. ..w...x...y...z...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4FFCC0C1-FAE9-48A2-A197-5DE81C053074}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	0.8299261240595344
Encrypted:	false
SSDEEP:	3:vlFg7NNKElClDK/lFlpY/4wltfvauldl5l/Hbl5l/cE///TzNM/wPxZlhWu/m7NH:vlapUElClDK/KFlgELW/wPxZSudxZSuq
MD5:	82C21E9F7253A902ACA51C429967E6B0
SHA1:	9FA5A85CAA74390218B1C00A5361C91F82EAFD06
SHA-256:	0DC9AC96F8D916E28E48EDD9826229319C2CEA698101748FA4263C9C35E710D5
SHA-512:	20A6973CB188AA313DB8D9A0D54CF2FCB1F47375F72761E6753F88772F35C212C49CBB65ACF89FB74848237A3C3176D21D68DF5A391E4A8C2CF30DE7BA9CEC D
Malicious:	false
Preview:	../.....E.M.B.E.D. .P.a.c.k.a.g.e..... . ...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D9320A51-5E17-41AC-AA14-257027C1CCDA}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\a0v2H8.jar

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	164473
Entropy (8bit):	**7.998227410119545**
Encrypted:	**true**
SSDEEP:	3072:nHtZMJGepfzX0wzh3ai4MhIcm3o9wpqmkAiye3Y6/tocHRXiIsWckuHvDdbFjW0V:nHtmJnbEwVak+5BoY6/KcWbog
MD5:	5FCE04720A34D47CE0D474F4571AE901
SHA1:	66F0FF1759880EE5AFC62968A4D135743A4B6888
SHA-256:	8CB74BD01205DF1E777CC8C1A343AA65287909CD72AA7B8388F4C32024DCE624
SHA-512:	6F0E3D750EFEB829E9CA00180AC0EF64B39A86A2B6BC6B087E917D65E89248EAB4CDB91EB2E81EF1144E799CB7186A26E947CB89044D3AD80A9606C600075E F7
Malicious:	**true**

Preview:	PK.....+U....~.....META-INF/MANIFEST.MF.M..LK-...K-*...R0.3..r.C.q,HL.HU...%...,x..s...u..K2.....].J.v.=.xc.C.$.K.....T.....y..\...y.`#..|.|.r.3..<y.x..PK.....+U;EC.. @...r.....uBT1nphWVB.class.}.\TG.xu..f.`f.A..o....O./...Q..AE...hN../.4*.x!..>.(*.dc..$.....$..9.w.{o.....}.~B.....|...2..G. 0.....pnlL....}^....isz..&,^.....!.A..iu..~#..-J.2....FK .8....7m..p.....3.g.&.....97=i..9g^..1..,O.F..\....{t..Q..Y.%..Q#.ED..*..a.....6.U.....1.....C-KI.=2%59"m.L.89a.k..`..>..eN.....F>.,u..>....5*)iJtf.8..0p..y..#.....'n..~..Cr...Q.1 ..H.n1...l#..J^....&.C..'A.t.3.).....%.Hl.`...'..S.ehOk.....t....F..zf"...gb.%}.RF!.X.b_E.K.7..[.....{e.*...l.9Pr....ug..A.tY....d.E.k#..O.GgsP...d.>.`.....6...w.S.{.....y.....+[YYx. wy.wY.@ ..W.{...uk....We..+[WYx.f.....5.V.^....{k..Te..+[UYx.f.....>]...xIkn..=w{..[k.VWe].W....b.....>Y....y.=...oo<.{..._YXT.e.....u.....Yz{cA.....UYe..r*..k.l.9p...K..(..kn...k..-..z

C:\Users\user\AppData\Local\Temp\a0v2H8.jar:Zone.Identifier

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E 98
Malicious:	false
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\12-09-2022 S#U0130PAR#U0130#U015e.docx.LNK

Process:	C:\Program Files\Microsoft Office\Office14\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 15:45:52 2022, mtime=Tue Mar 8 15:45:52 2022, atime=Mon Sep 12 19:45:10 2022, length=258604, window=hide
Category:	dropped
Size (bytes):	1154
Entropy (8bit):	4.508288966876625
Encrypted:	false
SSDEEP:	24:8GJ/XThOxqu/xfblueQ8DdNAlZDv3qIu7D:8GJ/XT4xjxfbQ18AyI0D
MD5:	03CDF502971DEBC9402065E8991080CB
SHA1:	A43BC44AA0394871BDDAAF05EE16119775EAE103
SHA-256:	AD1C2338FE7FCF5BEC6158C701A16F5EEBAB8A0EC754EB1A96D7014366C8A5D6
SHA-512:	FDB1316DCD2339EAD41163923DE0617109EA1F5D9C717FDB1D562D254E2BC1863F82169A43FD5ECB21C2608D75CBAD28B4F54B7F3A447D241702A377D9F771 0
Malicious:	false
Preview:	L.....F.... ...z.V..3..z.V..3..x.....,.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,- .2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....hT....Desktop.d.....QK.XhT..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2 .1.7.6.9.....2.,...,U.. .12-09-~1.DOC.....hT..hT..*...r.....'.....1.2.-.0.9.-.2.0.2.2. .S.#.U.0.1.3.0.P.A.R.#.U.0.1.3.0.#.U.0.1.5.e...d.o.c.x...d.o.c.....-...8...[... .....?J.....C:\Users\..#.....\\936905\Users.user\Desktop\12-09-2022 S#U0130PAR#U0130#U015e.docx.doc.A.....\.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.1.2.-.0.9.-.2 .0.2.2. .S.#.U.0.1.3.0.P.A.R.#.U.0.1.3.0.#.U.0.1.5.e...d.o.c.x...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	127
Entropy (8bit):	4.825539665366856
Encrypted:	false
SSDEEP:	3:bDuMJltcuHQ+S19gUPLFSmX1UXBuHQ+S19gUPLFSv:bCYc6sRzFGXB6sRzFc
MD5:	CD2C2025F8A0A79B19C38C6E5471BF29
SHA1:	14CBE217A0F3E0328FA0C8832123C09FCB715CBB
SHA-256:	8B250686B3B3AAD7A382D06FCA7D7F3C3BD334D5A24A1C2B9D7A0F1ADFAC1A62
SHA-512:	D113D6ADED11C44F2DB0EC7CF374F7BB51316C2D4AE7FF4F023BAE1EA79F1F6ECA2586F6834EA08B066C4C22DEA6F5DF52A80AAB4502A45820C222F628CD8 D76
Malicious:	false
Preview:	[folders]..Templates.LNK=0..12-09-2022 S#U0130PAR#U0130#U015e.docx.LNK=0..[doc]..12-09-2022 S#U0130PAR#U0130#U015e.docx.LNK=0..

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h....z.....p4h....x...

C:\Users\user\Desktop\~$-09-2022 S#U0130PAR#U0130#U015e.docx.doc

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h....z.....p4h....x...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.97914499665771
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:	12-09-2022 S#U0130PAR#U0130#U015e.docx.doc
File size:	258604
MD5:	7e8133cf5f56adcfafb9bc91390c9fe7
SHA1:	2cc6471245901e51565ad69df6b8586629965cf1
SHA256:	7859fd95c60a0d76fa99eb42277501b20f76a377c1395b504acff5dd22533027
SHA512:	943c44eb826863181891fa7f3eaba59546656c10aad65815f9a21d0ac277d21ec3715f71b1359b962c2057ee234f16be2edc0629e6a5889ff1abd4d2fd1f6d67
SSDEEP:	6144:CsjU1vruW+UztmXtb2wDayQ7B4Y6/EcKbiCW:tjaumMXtb2w+yM4YhVWCW
TLSH:	09442358C8204D84D8654636A8A9B9F392EF9020B322C11B7F5CC6EDDF6272E47AE513
File Content Preview:	PK.....!.....T.....[Content_Types].xml ... (.....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/701320/sample/12-09-2022 S#U0130PAR#U0130#U015e.docx.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:	False

Summary	
Author:	
Template:	
Last Saved By:	
Revion Number:	1
Total Edit Time:	1
Create Time:	2022-09-11T20:26:00Z
Last Saved Time:	2022-09-11T20:27:00Z
Number of Pages:	1
Number of Words:	3
Number of Characters:	21
Creating Application:	
Security:	0

Document Summary	
Number of Lines:	1
Number of Paragraphs:	1
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	14.0000

Streams	
Stream Path: \x1CompObj, File Type: data, Stream Size: 72	
General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	72
Entropy:	3.8231129765226823
Base64 Encoded:	False
Data ASCII:	. . . . . . / . { . . . Z @ . . . . P a c k a g e . . . . . P a c k a g e . 9 q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 a7 0d f2 2f c0 ce 11 92 7b 08 00 09 5a e3 40 08 00 00 00 50 61 63 6b 61 67 65 00 00 00 00 00 08 00 00 00 50 61 63 6b 61 67 65 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x10le, File Type: data, Stream Size: 20	
General	
Stream Path:	\x1Ole
File Type:	data
Stream Size:	20
Entropy:	0.8475846798245739
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	01 00 00 02 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x10le10Native, File Type: data, Stream Size: 165046

General	
Stream Path:	\x1Ole10Native
File Type:	data
Stream Size:	165046
Entropy:	7.9974019330364134
Base64 Encoded:	True
Data ASCII:	. . . . a 0 v 2 H 8 . j a r . C : \\ U s e r s \\ M I C R O S O F T \\ A p p D a t a \\ L o c a l \\ M i c r o s o f t \\ W i n d o w s \\ I N e t C a c h e \\ C o n t e n t . W o r d \\ a 0 v 2 H 8 . j a r . . . . . W . . . C : \\ U s e r s \\ M I C R O S ~ 1 \\ A p p D a t a \\ L o c a l \\ T e m p \\ { 6 1 6 8 B 7 1 6 - 2 6 0 4 - 4 F 6 B - B 0 F 1 - C C A D 4 0 6 6 7 2 3 F } \\ a 0 v 2 H 8 . j a r . y . . P K . . . . . + U ~ . . . . . M E T A - I N F / M A N I F E S T . M F M L K - . . K - * . R 0 3 r
Data Raw:	b2 84 02 00 02 00 61 30 76 32 48 38 2e 6a 61 72 00 43 3a 5c 55 73 65 72 73 5c 4d 49 43 52 4f 53 4f 46 54 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 49 4e 65 74 43 61 63 68 65 5c 43 6f 6e 74 65 6e 74 2e 57 6f 72 64 5c 61 30 76 32 48 38 2e 6a 61 72 00 00 00 03 00 57 00 00 00 43 3a 5c 55 73 65 72 73 5c 4d 49 43 52 4f 53 7e 31 5c

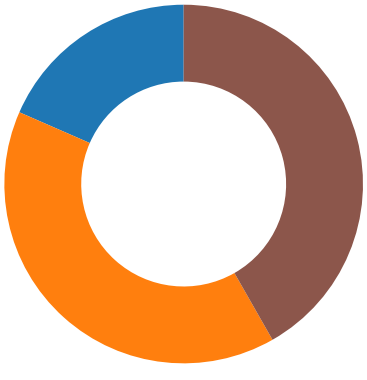
Stream Path: \x3ObjInfo, File Type: data, Stream Size: 6	
General	
Stream Path:	\x3ObjInfo
File Type:	data
Stream Size:	6
Entropy:	1.7924812503605778
Base64 Encoded:	False
Data ASCII:	@ . . . . .
Data Raw:	40 00 03 00 01 00

Network Behavior

No network behavior found

Statistics

Behavior



- WINWORD.EXE
- javaw.exe
- WMIC.exe
- WMIC.exe
- WMIC.exe
- javaw.exe
- WMIC.exe
- WMIC.exe
- WMIC.exe
- WMIC.exe
- WMIC.exe

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1216, Parent PID: 576

General	
Target ID:	0
Start time:	13:45:10

Start date:	12/09/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13fcc0000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E21A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E21A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E21A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E240648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E240648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E240648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\6DAA6	success or wait	1	6E240648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\6DAA6	6DAA6	binary	04 00 00 00 C0 04 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 EE 6B 08 A2 E8 C6 D8 01 A6 DA 06 00 A6 DA 06 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6E240648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\6DAA6	6DAA6	binary	04 00 00 00 C0 04 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00	04 00 00 00 C0 04 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67	success or wait	1	6E240648	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			EE 6B 08 A2 E8 C6 D8 01 A6 DA 06 00 A6 DA 06 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 73 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A6 DA 06 00 A6 DA 06 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
				00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: javaw.exe PID: **1952**, Parent PID: **1216**

General

Target ID:	3
Start time:	13:45:36
Start date:	12/09/2022
Path:	C:\Program Files\Java\jre1.8.0_121\bin\javaw.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Java\jre1.8.0_121\bin\javaw.exe" -jar "C:\Users\user\AppData\Local\Temp\a0v2H8.jar"
Imagebase:	0x13f680000
File size:	206912 bytes
MD5 hash:	7F0467C3AA5BDAF44BBC824AC81359D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Java
Yara matches:	• Rule: JoeSecurity_AdWind_2, Description: Yara detected AdWind RAT, Source: 00000003.00000002.1046522557.00000000D747C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AdWind_2, Description: Yara detected AdWind RAT, Source: 00000003.00000002.1045659100.00000000D7407000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hsperfdata_user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA9DF40	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\hsperfdata_user\1952	read attributes | delete | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file | delete on close	success or wait	1	6DA9E09F	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7c05.timestamp	0	51	43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 4a 61 76 61 5c 6a 72 65 31 2e 38 2e 30 5f 31 32 31 0d 0a 31 36 36 33 30 31 35 35 35 31 39 39 30 0d 0a	C:\Program Files\Java\jre1.8.0_1211663015551990	success or wait	1	73C1CB65	WriteFile
unknown	unknown	2			invalid handle	2	73C1CB65	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\a0v2H8.jar	unknown	22	success or wait	1	13F69873D	ReadFile
C:\Users\user\AppData\Local\Temp\a0v2H8.jar	unknown	1024	success or wait	1	13F69873D	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\amd64\jvm.cfg	unknown	4096	success or wait	1	13F69873D	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\amd64\jvm.cfg	unknown	4096	end of file	1	13F69873D	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\meta-index	unknown	4096	success or wait	1	6D860516	unknown
C:\Program Files\Java\jre1.8.0_121\lib\meta-index	unknown	4096	end of file	1	6D860756	unknown
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	4	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	128	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	97	success or wait	3	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	15	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\ext\meta-index	unknown	8192	success or wait	1	73C1CB24	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\ext\meta-index	unknown	8192	end of file	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	1	73C1CB24	ReadFile
C:\Users\user\AppData\Local\Temp\a0v2H8.jar	unknown	4	success or wait	2	73C1CB24	ReadFile
C:\Users\user\AppData\Local\Temp\a0v2H8.jar	unknown	160	success or wait	10	73C1CB24	ReadFile
C:\Users\user\AppData\Local\Temp\a0v2H8.jar	unknown	30	success or wait	9	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	208	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\meta-index	unknown	8192	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\meta-index	unknown	8192	end of file	1	73C1CB24	ReadFile
C:\Users\user\AppData\Local\Temp\a0v2H8.jar	unknown	1024	success or wait	159	73C1CB24	ReadFile
C:\Users\user\AppData\Local\Temp\a0v2H8.jar	unknown	1024	end of file	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\resources.jar	unknown	4	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\resources.jar	unknown	128	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\accessibility.properties	unknown	8192	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\accessibility.properties	unknown	8192	end of file	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	1	73C1CB24	ReadFile
\pipe	unknown	8192	success or wait	6	73C1CB24	ReadFile
\pipe	unknown	8192	pipe broken	3	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\security\java.security	unknown	8192	success or wait	5	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\security\java.security	unknown	8192	end of file	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\jsse.jar	unknown	4	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\jsse.jar	unknown	128	success or wait	1	73C1CB24	ReadFile

Analysis Process: WMIC.exe PID: **2452**, Parent PID: **1952**

General

Target ID:	4
Start time:	13:45:40
Start date:	12/09/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic CPU get ProcessorId
Imagebase:	0xff5a0000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WMIC.exe PID: **2308**, Parent PID: **1952**

General

Target ID:	6
Start time:	13:45:46
Start date:	12/09/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false

Commandline:	wmic bios get serialnumber
Imagebase:	0xff4f0000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WMIC.exe PID: **772**, Parent PID: **1952**

General

Target ID:	8
Start time:	13:45:49
Start date:	12/09/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic csproduct get name
Imagebase:	0xff970000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: javaw.exe PID: **1316**, Parent PID: **1216**

General

Target ID:	10
Start time:	13:45:50
Start date:	12/09/2022
Path:	C:\Program Files\Java\jre1.8.0_121\bin\javaw.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Java\jre1.8.0_121\bin\javaw.exe" -jar "C:\Users\user\AppData\Local\Temp\a0v2H8.jar"
Imagebase:	0x13f680000
File size:	206912 bytes
MD5 hash:	7F0467C3AA5BDAF44BBC824AC81359D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AdWind_2, Description: Yara detected AdWind RAT, Source: 0000000A.00000002.1107491922.00000000D7403000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AdWind_2, Description: Yara detected AdWind RAT, Source: 0000000A.00000002.1108130731.00000000D7479000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hsperfdata_user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA9DF40	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\hsperfdata_user\1316	read attributes | delete | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file | delete on close	success or wait	1	6DA9E09F	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7c05.timestamp	0	51	43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 4a 61 76 61 5c 6a 72 65 31 2e 38 2e 30 5f 31 32 31 0d 0a 31 36 36 33 30 31 35 35 35 31 39 39 30 0d 0a	C:\Program Files\Java\jre1.8.0_1211663015551990	success or wait	1	73C1CB65	WriteFile
unknown	unknown	2			invalid handle	2	73C1CB65	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\a0v2H8.jar	unknown	22	success or wait	1	13F69873D	ReadFile
C:\Users\user\AppData\Local\Temp\a0v2H8.jar	unknown	1024	success or wait	1	13F69873D	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\amd64\jvm.cfg	unknown	4096	success or wait	1	13F69873D	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\amd64\jvm.cfg	unknown	4096	end of file	1	13F69873D	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\meta-index	unknown	4096	success or wait	1	6D860516	unknown
C:\Program Files\Java\jre1.8.0_121\lib\meta-index	unknown	4096	end of file	1	6D860756	unknown
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	4	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	128	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	97	success or wait	3	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	15	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	62	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\ext\meta-index	unknown	8192	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\ext\meta-index	unknown	8192	end of file	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	1	73C1CB24	ReadFile
C:\Users\user\AppData\Local\Temp\a0v2H8.jar	unknown	4	success or wait	2	73C1CB24	ReadFile
C:\Users\user\AppData\Local\Temp\a0v2H8.jar	unknown	160	success or wait	10	73C1CB24	ReadFile
C:\Users\user\AppData\Local\Temp\a0v2H8.jar	unknown	30	success or wait	9	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	207	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\meta-index	unknown	8192	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\meta-index	unknown	8192	end of file	1	73C1CB24	ReadFile
C:\Users\user\AppData\Local\Temp\a0v2H8.jar	unknown	1024	success or wait	161	73C1CB24	ReadFile
C:\Users\user\AppData\Local\Temp\a0v2H8.jar	unknown	1024	end of file	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\resources.jar	unknown	4	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\resources.jar	unknown	128	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\accessibility.properties	unknown	8192	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\accessibility.properties	unknown	8192	end of file	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	8059	success or wait	48	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	1	73C1CB24	ReadFile
\pipe	unknown	8192	success or wait	5	73C1CB24	ReadFile
\pipe	unknown	8192	pipe broken	3	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\security\java.security	unknown	8192	success or wait	5	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\security\java.security	unknown	8192	end of file	1	73C1CB24	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\Java\jre1.8.0_121\lib\jsse.jar	unknown	4	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\jsse.jar	unknown	128	success or wait	1	73C1CB24	ReadFile
C:\Program Files\Java\jre1.8.0_121\lib\rt.jar	unknown	160	success or wait	16	73C1CB24	ReadFile

Analysis Process: WMIC.exe PID: **1916**, Parent PID: **1952**

General

Target ID:	11
Start time:	13:45:52
Start date:	12/09/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic csproduct get UUID
Imagebase:	0xff4a0000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WMIC.exe PID: **2016**, Parent PID: **1316**

General

Target ID:	13
Start time:	13:45:56
Start date:	12/09/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic CPU get ProcessorId
Imagebase:	0xff920000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WMIC.exe PID: **2344**, Parent PID: **1316**

General

Target ID:	15
Start time:	13:46:08
Start date:	12/09/2022

Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic bios get serialnumber
Imagebase:	0xff3b0000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WMIC.exe PID: **316**, Parent PID: **1316**

General

Target ID:	17
Start time:	13:46:13
Start date:	12/09/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic csproduct get name
Imagebase:	0xff880000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WMIC.exe PID: **2496**, Parent PID: **1316**

General

Target ID:	19
Start time:	13:46:17
Start date:	12/09/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic csproduct get UUID
Imagebase:	0xffd70000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly