

ID: 355599
Sample Name:
SecuriteInfo.com.Exploit.Siggen3.10350.27303.12062
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 02:06:08
Date: 20/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report SecuriteInfo.com.Exploit.Siggen3.10350.27303.12062 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
System Summary: 4
Signature Overview 5
AV Detection: 5
Compliance: 5
Software Vulnerabilities: 5
System Summary: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 13
General 13
File Icon 13
Static OLE Info 13
General 14
OLE File "SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls" 14
Indicators 14
Summary 14
Document Summary 14
Streams 14
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 14
General 14
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 14
General 14

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 157800 15
General 15
Macro 4.0 Code 15
Network Behavior 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 16
DNS Queries 16
DNS Answers 16
HTTP Request Dependency Graph 16
HTTP Packets 16
Code Manipulations 16
Statistics 16
Behavior 16
System Behavior 17
Analysis Process: EXCEL.EXE PID: 1748 Parent PID: 584 17
General 17
File Activities 17
File Created 17
File Deleted 18
File Moved 18
File Written 19
File Read 24
Registry Activities 24
Key Created 24
Key Value Created 25
Analysis Process: rundll32.exe PID: 2728 Parent PID: 1748 33
General 33
File Activities 34
Disassembly 34
Code Analysis 34

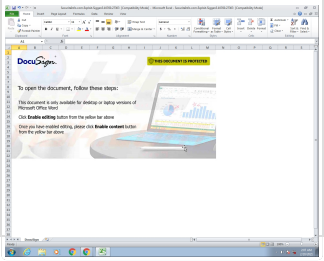
Analysis Report SecuriteInfo.com.Exploit.Siggen3.1035…

Overview

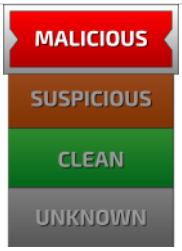
General Information

Sample Name:	SecuriteInfo.com.Exploit.Siggen3.10350.27303.12062 (renamed file extension from 12062 to xls)
Analysis ID:	355599
MD5:	ad9550ee6ece83..
SHA1:	d0617e5cb90b4d..
SHA256:	74423c8236cd50..

Most interesting Screenshot:



Detection



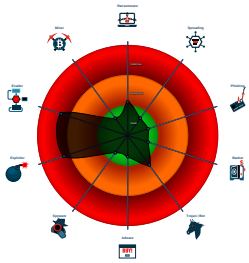
Hidden Macro 4.0

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Allocates a big amount of memory (p…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Potential document exploit detected…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1748 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2728 cmdline: rundll32 ..\BASE.BABAA,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.Siggen3.10350.27303.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

Sigma Overview

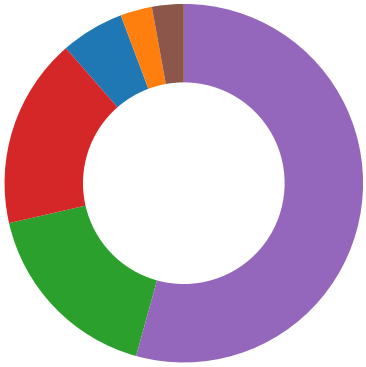
System Summary:



Sigma detected: Microsoft Office Product Spawning Windows Shell

Copyright null 2021

Signature Overview



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

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

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

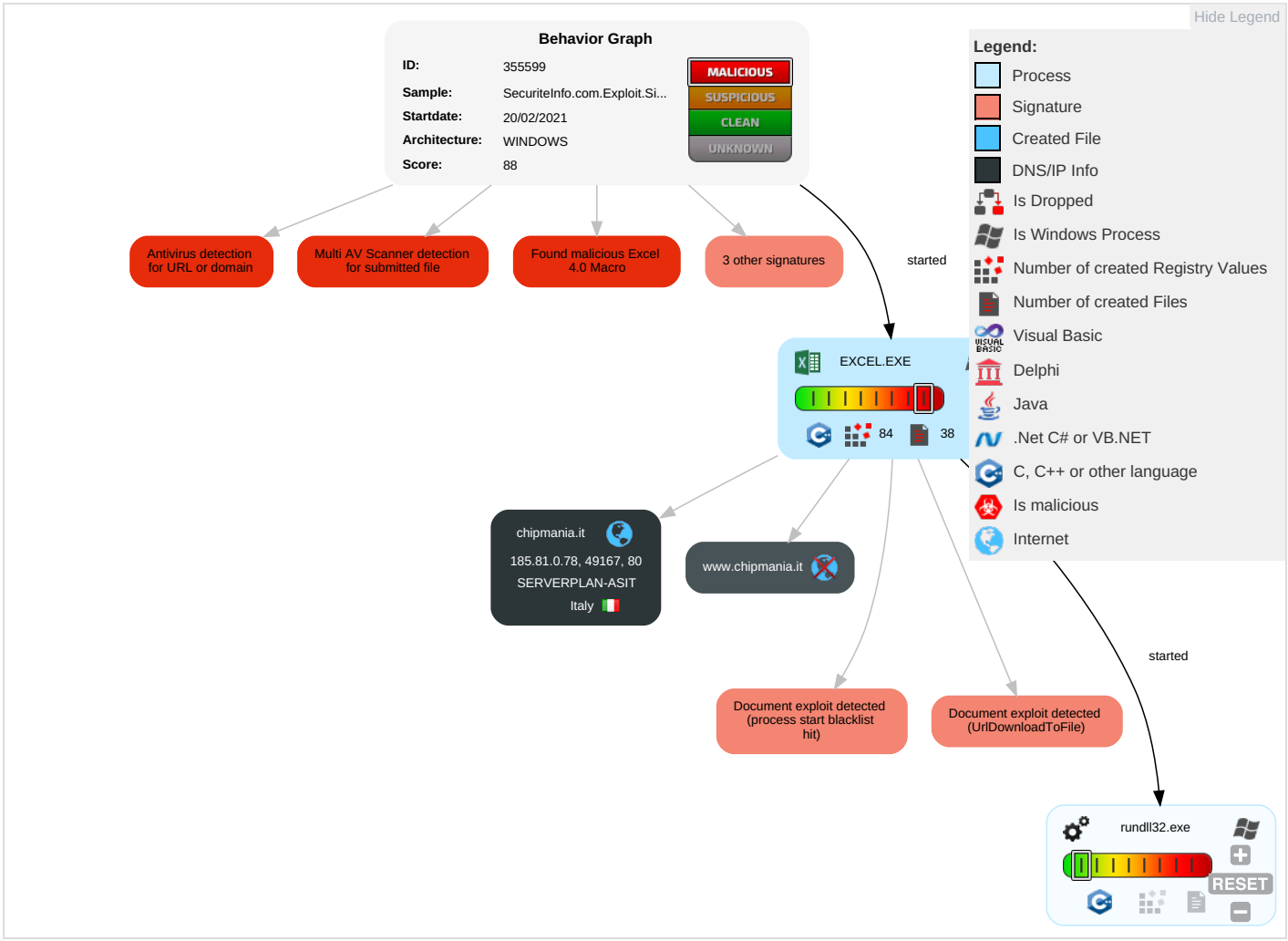
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Copyright null 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Extra Window Memory Injection 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

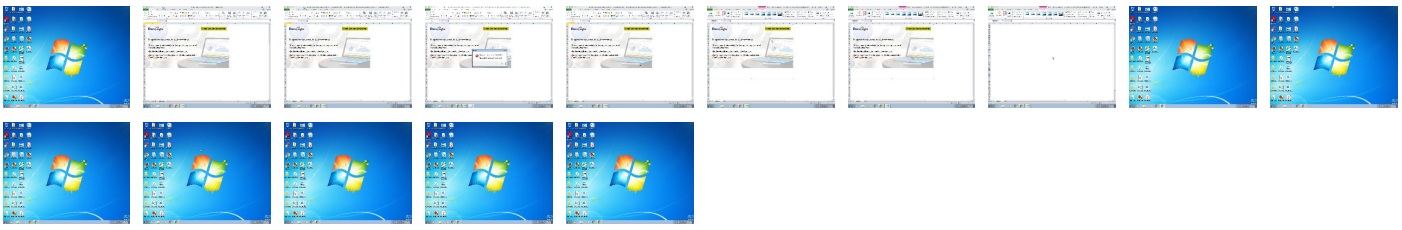
Behavior Graph

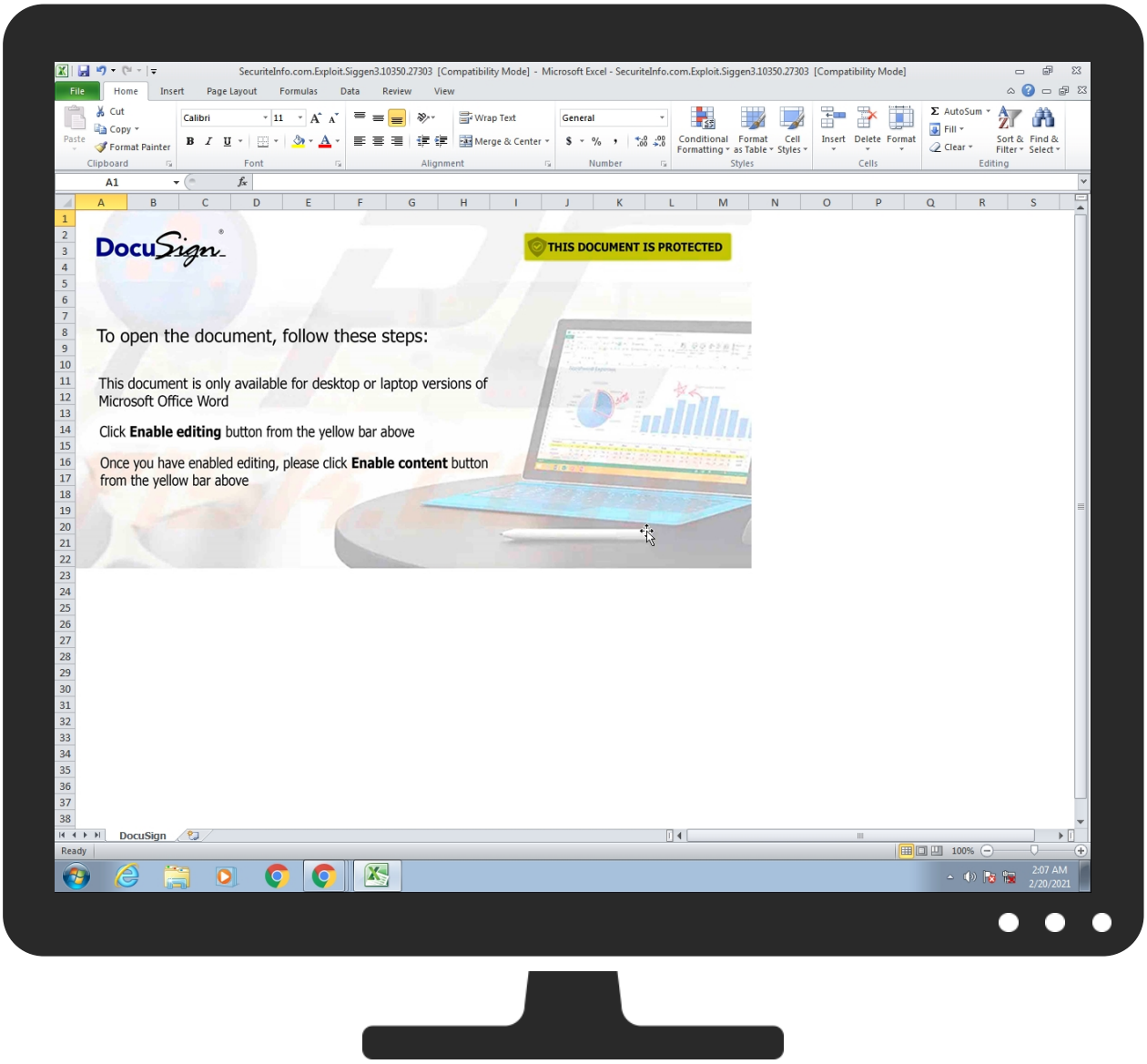


Screenshots

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.Siggen3.10350.27303.xls	11%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

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://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://www.chipmania.it/mails/open.php	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.chipmania.it/mails/open.php	true	• 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, 00000003.0000000 2.2148203075.0000000001E37000. 00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000003.0000000 2.2148054390.0000000001C50000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2148054390.0000000001C50000. 00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2148054390.0000000001C50000. 00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2148203075.0000000001E37000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2148203075.0000000001E37000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2148054390.0000000001C50000. 00000002.00000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2148054390.0000000001C50000. 00000002.00000001.sdmp	false		high

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355599
Start date:	20.02.2021
Start time:	02:06:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.Siggen3.10350.27303.12062 (renamed file extension from 12062 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:	6
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:	mal88.expl.evad.winXLS@3/5@1/1
EGA Information:	Failed

Copyright null 2021

HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

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

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php
	Sign-707465831_1420670581.xls	Get hash	malicious	Browse	• www.chipmania.it/mails/open.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SERVERPLAN-ASIT	SecuriteInfo.com.Exploit.Siggen3.10350.26515.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10350.31033.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.1476.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.1181.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.21235.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.15875.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.2804.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Heur.18554.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-636.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-92793351_1597657581.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-979329054_1327186231.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• 185.81.0.78
	Sign-707465831_1420670581.xls	Get hash	malicious	Browse	• 185.81.0.78
	SecuriteInfo.com.Exploit.Siggen3.10048.21670.xls	Get hash	malicious	Browse	• 93.95.216.145

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\3CCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	155530
Entropy (8bit):	7.660584123957991
Encrypted:	false
SSDEEP:	3072:YxWVpupSzxNEBBD+Os7/xxkKCtRbsYO1entseoXXj:YEGSzx0dmxk7RbsYsKtseoXT

C:\Users\user\AppData\Local\Temp\3CCE0000	
MD5:	C44E2E9FEFA57B31CDEFC8D201D895B5
SHA1:	6507ACF9CFBF7142AD5696253F3ABC300BB662CE
SHA-256:	9D1BC9044DB37900099FC4CB51160F6EA2C9A34D19ABEC0219F134C762991BE4
SHA-512:	D1C34695305599BDD43B280720D2AAA4E5C5DDC4A5B41449E85F16895D85C9474982D1F88254CD153D66B2A07C3F1B3E7AA48D0B4FE457F590059F01B45ECFC
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 09:06:38 2021, atime=Sat Feb 20 09:06:38 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.488986575688329
Encrypted:	false
SSDEEP:	12:85QUNcLgXg/XAlCPCHaXtB8XzB/KPaUX+WnicvbwbDtZ3YilMMEpxRljK6TdJP9O:85jNK/XTd6jASUYegDv3qfrNru/
MD5:	781443D351DE3D8B9E000C3D089898F3
SHA1:	7AE6978567BD588E9117BA9E8EC200331B4714AA
SHA-256:	EF036CCC61EFD384EB738CB22440DA9C5E95B4CB67C72B5FB430D55034011F7D
SHA-512:	C43F4F27886E9B341A186F28750D85A6117902945603142928AD61BD1686D1D086788964118300881045 4D4E435F40CEDAB29C67FC16E24C88702114343D3802
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G.....p.....p.... .....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.P..Desktop.d.....QK.XTR.P*..._=.....:.....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\..#.....\\688098\Users.user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L 8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....688098.....D_....3N...W...9r.[.*.....}EkD_....3N.. .W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.Siggen3.10350.27303.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 09:06:25 2021, mtime=Sat Feb 20 09:06:38 2021, atime=Sat Feb 20 09:06:38 2021, length=168448, window=hide
Category:	dropped
Size (bytes):	2368
Entropy (8bit):	4.569920188815355
Encrypted:	false
SSDEEP:	48:8HAd/XT0jxHC31qHClfQh2HAd/XT0jxHC31qHClfQ/:8HG/XojxitlfQh2HG/XojxitlfQ/
MD5:	FC67E56CC21CA04C73C4B56C9D1B47FF
SHA1:	ADEA14F4591F2632F89A83ED1045502CB94FD043
SHA-256:	D6F94A6DFDE437561339F3F912B8D14674425D9A646A914197EF1F0BD25F9010
SHA-512:	212BA29FB7714D1D43FA97EDC52453DED1301CF57A6E9B45EE898C8E5A39E0CA9DCAB706D7DD829BAC52ACD03C9914EEC8EA0893E30E678734C72F7A76A40 5E
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...u...p.....p....S..p.....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.P..Desktop.d.....QK.XTR.P*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-2 .1.7.6.9.....2.....TR.P .SECURI~1.XLS.....TR.PTR.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...2.7.3.0.3...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\688098\Users.user\Desktop\SecuriteInfo.com.Exploit.Siggen3.10350.27303.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...2.7.3.0.3...x.l.s.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	185
Entropy (8bit):	4.833884412063983
Encrypted:	false
SSDEEP:	3:oyBVomM0bcsoMW/SWCuscbcsoMW/SWCmM0bcsoMW/SWCv:dj60wsoMWKW7wsoMWKWU0wsoMWKWs
MD5:	8008051768264A8F63462178EE0A3809
SHA1:	2FA73992D0C2D6C872FF64374034E841D3BB0CAA
SHA-256:	57612946322F859DBB4A3CEF93B041BA8F62C0BC4252DB26A95F8EE72A64CF32

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA-512:	F054CBE1CA26C4C63742A29E28FF8D183349875863887E2EEEA4EEF42191F29F5B36DEAD52CB394524A97FD3E56D0172D7EF27F44807B19206B5A666C4D988AE
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..SecuriteInfo.com.Exploit.Siggen3.10350.27303.LNK=0..SecuriteInfo.com.Exploit.Siggen3.10350.27303.LNK=0..[xls]..SecuriteInfo.com.Exploit.Siggen3.10350.27303.LNK=0..

C:\Users\user\Desktop\4FCE0000	
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):	7.239939186555363
Encrypted:	false
SSDEEP:	3072:zccKoSsxzNDZLDZjlbR868O8KL5L+4iK2xEtjPOtioVjDGUU1qfDlaGGx+cL2Qn8:4cKoSsxzNDZLDZjlbR868O8KL5L+4iKo
MD5:	55BB2085B17B24C9047A18CAB0FEDBAB
SHA1:	CE0E5D44B46F4517000E492D307E49280220CFEA
SHA-256:	16A11EE385E26D296DA33E0D46AB9D4F18C9DE51088D8D14B9A13D8C0913A603
SHA-512:	2C2EA2C4952C74726EE9304AE9719F7858A888FE6CE9F45A619033C09CB36DCEDAB00B9091A43858316C85BEC7A8CD5BB70C689CCD282BB4C19831998CE89E7
Malicious:	false
Reputation:	low
Preview:	........g2.....\.p.... B.....a.....=.....=.....i..9J.8.....X.@.....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1...,..8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Fri Feb 19 10:48:36 2021, Security: 0
Entropy (8bit):	7.195176543915214
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	SecuriteInfo.com.Exploit.Siggen3.10350.27303.xls
File size:	168960
MD5:	ad9550ee6ece8322501ed92d374d3928
SHA1:	d0617e5cb90b4db4fcf2269ffd8228b9ca4f89af
SHA256:	74423c8236cd5057af8e4ffbf84fdcbb34f5e6dc8f8dc0520c685c7fd6bc100a
SHA512:	531ab2de644449e17e4f6d4a708f98a89bd6ac972b0bc6ed6b725205e5a0412ef6b0dfa9bdb422f6732c5396b8d0c82783c88c3727496488c71cb960b25d2f0b
SSDEEP:	3072:bScKoSsxzNDZLDZjlbR868O8KlVH3jiKq7uDphYHceXVhca+fMHLtyeGxcl8OUMj:OcKoSsxzNDZLDZjlbR868O8KlVH3jiK+
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.Siggen3.10350.27303.xls"

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

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

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

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.357299206868
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . D o c u S i g n . . . . . D o c u S i g n . . . . . D o c u S i g n . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 ec 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 ac 00 00 00 02 00 00 00 e3 04 00 00

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

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

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 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

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2021 02:06:59.939125061 CET	52197	53	192.168.2.22	8.8.8.8
Feb 20, 2021 02:06:59.996273041 CET	53	52197	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 02:06:59.939125061 CET	192.168.2.22	8.8.8.8	0x71dd	Standard query (0)	www.chipmania.it	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 20, 2021 02:06:59.996273041 CET	8.8.8.8	192.168.2.22	0x71dd	No error (0)	www.chipmania.it	chipmania.it		CNAME (Canonical name)	IN (0x0001)
Feb 20, 2021 02:06:59.996273041 CET	8.8.8.8	192.168.2.22	0x71dd	No error (0)	chipmania.it		185.81.0.78	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.chipmania.it

HTTP Packets

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

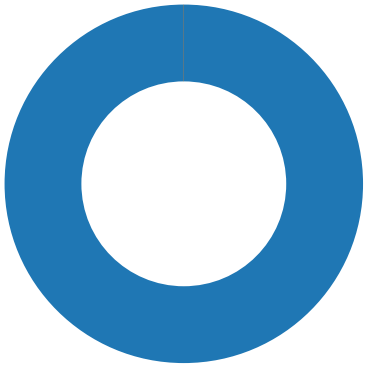
Timestamp	kBytes transferred	Direction	Data
Feb 20, 2021 02:07:00.080370903 CET	0	OUT	GET /mails/open.php HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: www.chipmania.it Connection: Keep-Alive

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1748 Parent PID: 584

General

Start time:	02:06:35
Start date:	20/02/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fd60000
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\CA13.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1400AEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\3CCE0000	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	140A8828C	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	140A8828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140A8828C	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	140A8828C	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	140A8828C	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	140A8828C	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	140A8828C	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	140A8828C	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	140A8828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\AF05.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1400AEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CA13.tmp	success or wait	1	14031B818	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\AF05.tmp	success or wait	1	14031B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3CCE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\4FCE0000	C:\Users\user\Desktop\SecuriteInfo.com.Exploit.Siggen3.10350.27303.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

Copyright null 2021

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEA859AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3CCE0000	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\3CCE0000	1022	2	03 00	..	success or wait	22	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\3CCE0000	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\3CCE0000	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\3CCE0000	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 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 c6 33 e4 6d 20 01 00 00 c2 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 26 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 6f 40 54 27 ac 01 00 00 0c 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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/.relsPK..-.....!..3.m ....&...xl/_rels/workbook.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\4FCE0000	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 00 20 20 20

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\4FCE0000	unknown	10137	49 ed 10 e0 c1 09 2d 0a 69 20 0e de 0f 0b e0 08 12 fa 42 5f 74 de f1 61 15 3d a9 0e 22 7d 02 5e e3 8d 3b 06 9b bf 81 af 0e 0c 13 5e 89 87 09 bf e9 1d dc 1b 2b af 95 0d d7 14 ff 00 73 61 1a 6d 69 a2 56 3a 49 b1 fd 5f 73 0e 22 7b 1b 3e 04 39 b2 1d ed 8d f8 70 03 f8 17 52 35 7f 48 a9 fc 85 3f 97 56 cd 29 15 89 fc ba a9 26 d9 b5 95 ce 9d 9e 33 b5 89 28 73 57 92 a8 ff 00 73 52 c6 96 11 df 33 af 75 55 77 6d fd ed de ef 8c ce 58 43 6c 66 14 40 b6 98 06 f9 cc eb 96 14 1b 49 89 54 6d 6d 46 fb 95 89 1c 49 4a 62 2b d2 d0 c5 63 7a 8e 26 da e1 d1 f1 62 ac 50 e8 4e 4c 7c cf 6d 57 e6 b4 90 2f 3e aa 88 0a 87 8d 2b 6e 6d 9f 2e de 47 b1 89 0b 52 f8 0f 36 70 b5 54 a8 f2 38 d0 2f f2 7f 22 25 59 d1 30 47 ca fc 1e 56 14 4d 51 54 96 7b 5b dd 4f 41 5a 0d 62 24 9b 49 e7 bb e8 a1	I.....-.i ....B_t..a.=..} .^..;.....^.....+..... sa.mi.V:I.._s."{.>.9.....p...R 5.H...?.V.).....&.....3..(sW. ...sR....3.uUwm.....XClf.@. .. ..I.TmmF....IJb+...cz.&... .b.P.NL|.mW.../>.....+nm... G.. .R..6p.T..8./.."%Y.0G...V.M QT.{[.OAZ.b$.I....	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\4FCE0000	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 00 20 20 20

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\4FCE0000	unknown	200	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 c0 7c 0d 23 d9 c6 01 40 00 00 00 00 0b c3 13 70 07 d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... @.....H.....T.....`..... ..x..... ....Microsoft Excel.@.....|.#... @.....p.....	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\4FCE0000	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 00 00 1e 10 00 00 03 00 00 00 0d 00 00 00 20 20 44 6f 63 75 53 69 67 6e 20 20 00 09 00 00 00 44 6f 63 75 53 69 67 6e 00 0a 00 00 00 44 6f 63 75 53 69 67 6e 20 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 01 00 00 00	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... DocuSign .....DocuSign..... DocuSign .....Work sheets.....	success or wait	1	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\4FCE0000	unknown	2048	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!...".#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\4FCE0000	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 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

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECA32	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECBE7	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECEF3	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECFCD	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\FB319	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\FB819	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\5795694722.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	3	7FEEA859AC0	unknown

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 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECA32	ECA32	binary	04 00 00 00 D4 06 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 B2 36 B2 0F 70 07 D7 01 32 CA 0E 00 32 CA 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECBE7	ECBE7	binary	04 00 00 00 D4 06 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 F8 17 2A 13 70 07 D7 01 E7 CB 0E 00 E7 CB 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00

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

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECEF3	ECEF3	binary	04 00 00 00 D4 06 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 8D 00 DF 13 70 07 D7 01 F3 CE 0E 00 F3 CE 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\ECFCD	ECFCD	binary	04 00 00 00 D4 06 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 32 00 37 00 33 00 30 00 33 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 D1 53 00 14 70 07 D7 01 CD CF 0E 00 CD CF 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	#)2	binary	23 29 32 00 D4 06 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 32 00 37 00 33 00 30 00 33 00 2E 00 78 00 6C 00 73 00 00 00 73 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 69 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 65 00 78 00 70 00 6C 00 6F 00 69 00 74 00 2E 00 73 00 69 00 67 00 67 00 65 00 6E 00 33 00 2E 00 31 00 30 00 33 00 35 00 30 00 2E 00 32 00 37 00 33 00 30 00 33 00 00 00	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FB319	FB319	binary	04 00 00 00 D4 06 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 2F 2B 9B 36 70 07 D7 01 19 B3 0F 00 19 B3 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00	success or wait	1	7FEEA859AC0	unknown

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

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FB819	FB819	binary	04 00 00 00 D4 06 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 2F 2B 9B 36 70 07 D7 01 19 B8 0F 00 19 B8 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:	0xffb60000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis