

JOeSandbox Cloud BASIC



ID: 403883

Sample Name: statistic-
2069354685.xlsm

Cookbook:
defaultwindowsofficecookbook.jbs

Time: 13:43:27

Date: 04/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report statistic-2069354685.xlsm	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
Software Vulnerabilities:	5
Networking:	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
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	12
Dropped Files	12
Created / dropped Files	13
Static File Info	18
General	18
File Icon	18
Static OLE Info	18
General	18
OLE File "statistic-2069354685.xlsm"	18
Indicators	18
Macro 4.0 Code	19
Network Behavior	19
TCP Packets	19
UDP Packets	20
DNS Queries	20
DNS Answers	20

HTTPS Packets	20
Code Manipulations	21
Statistics	21
Behavior	21
System Behavior	21
Analysis Process: EXCEL.EXE PID: 2116 Parent PID: 584	21
General	21
File Activities	22
File Created	22
File Deleted	23
File Moved	23
File Written	23
File Read	30
Registry Activities	30
Key Created	30
Key Value Created	30
Analysis Process: rundll32.exe PID: 2652 Parent PID: 2116	40
General	40
File Activities	41
Analysis Process: rundll32.exe PID: 2552 Parent PID: 2116	41
General	41
File Activities	41
File Read	41
Disassembly	41
Code Analysis	41

Analysis Report statistic-2069354685.xlsm

Overview

General Information

Sample Name:	statistic-2069354685.xlsm
Analysis ID:	403883
MD5:	e594ea809c24d8..
SHA1:	c402e78a57d801..
SHA256:	d328633005bb0fd.
Tags:	icedID xlm
Infos:	
Most interesting Screenshot:	

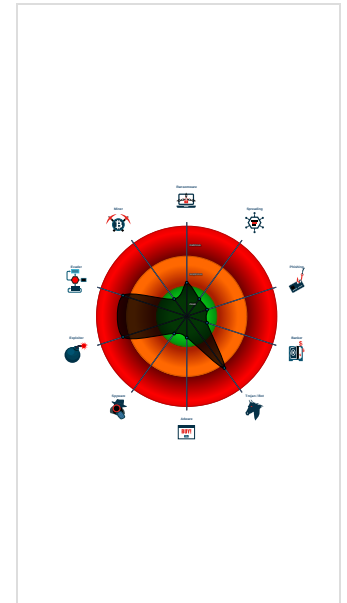
Detection

Hidden Macro 4.0	
Score:	84
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...
Sigma detected: System File Execu...
Yara detected MalDoc1
Excel documents contains an embe...
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: 2116 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
 - rundll32.exe (PID: 2652 cmdline: rundll32 ..\jordji.nbvt1,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
 - rundll32.exe (PID: 2552 cmdline: rundll32 ..\jordji.nbvt11,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
sharedStrings.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	

Sigma Overview

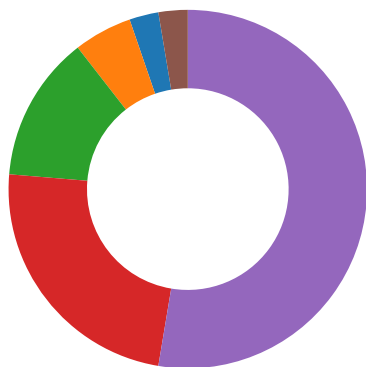
System Summary:



Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: System File Execution Location Anomaly

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Software Vulnerabilities:



Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:



Yara detected MalDoc1

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

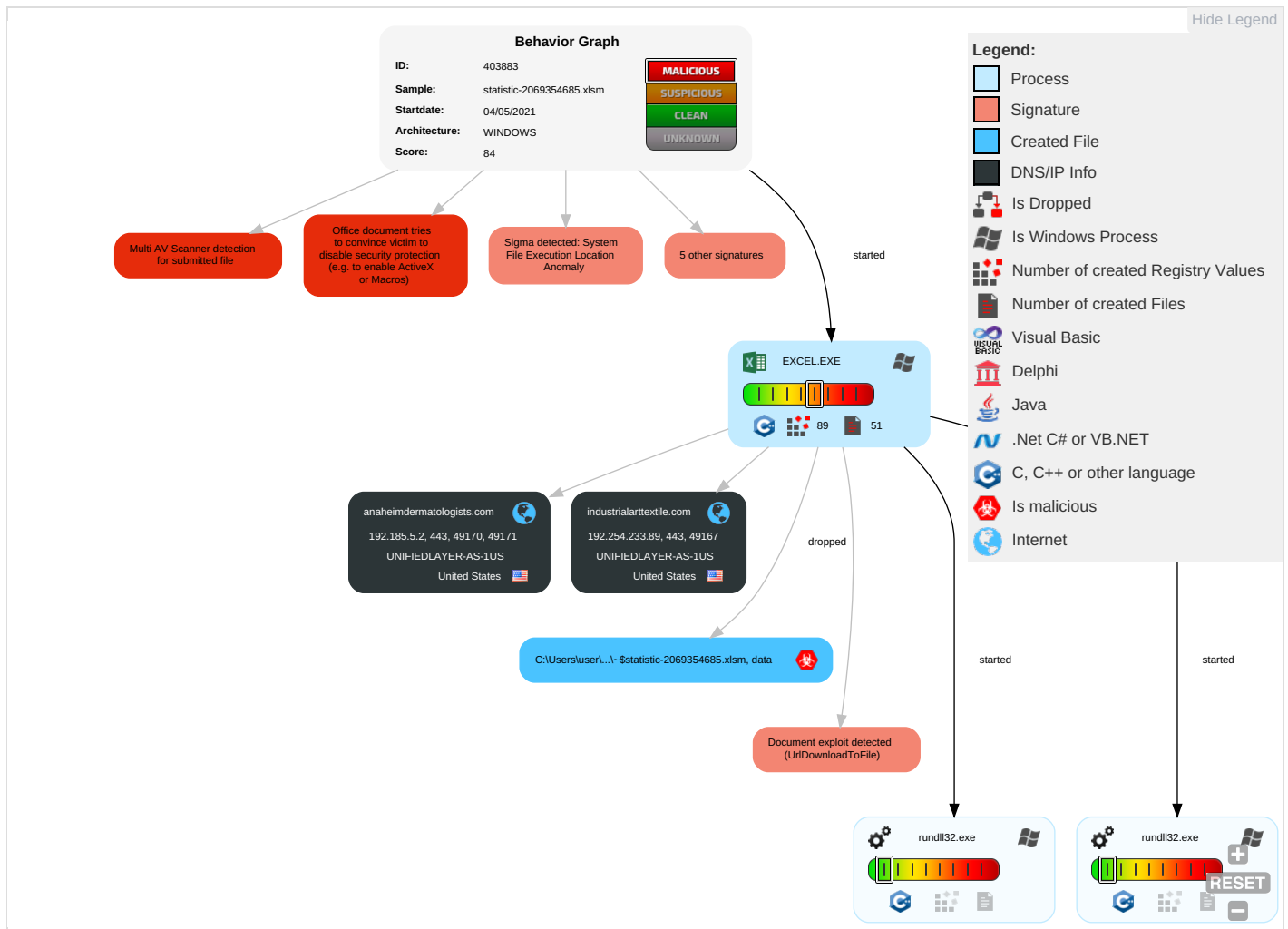
Found abnormal large hidden Excel 4.0 Macro sheet

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 21	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Rank or Rating

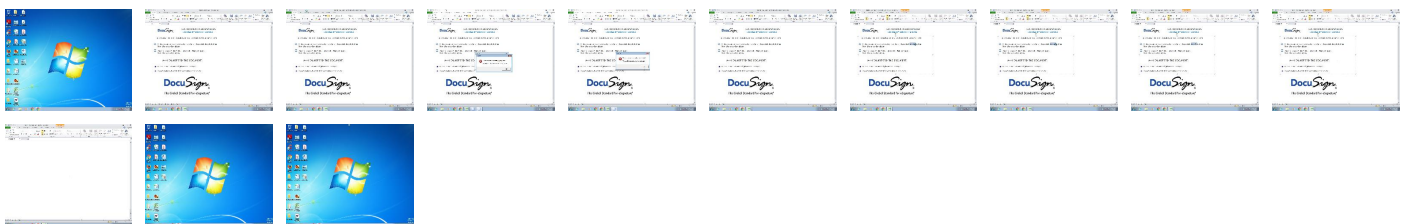
Behavior Graph

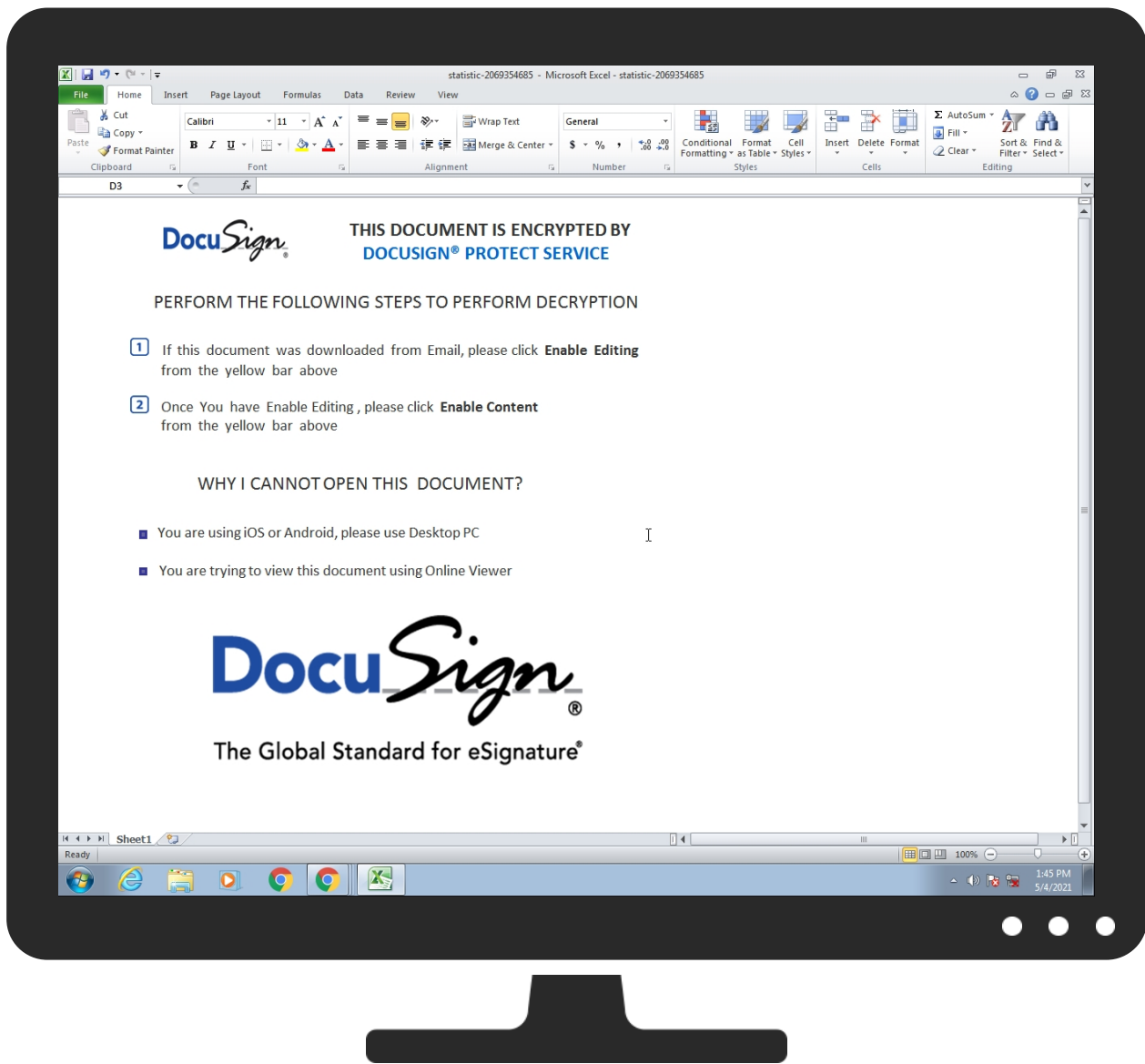


Screenshots

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
statistic-2069354685.xlsm	7%	Virustotal		Browse
statistic-2069354685.xlsm	21%	Metadefender		Browse
statistic-2069354685.xlsm	34%	ReversingLabs	Document-Office.Downloader.EncDoc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
anaheimdermatologists.com	3%	Virustotal		Browse
industrialarttextile.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	
http://www.icra.org/vocabulary/ .	0%	URL Reputation	safe	
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	
http://windowsmedia.com/redirect/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
anaheimdermatologists.com	192.185.5.2	true	false	3%, Virustotal, Browse	unknown
industrialarttextile.com	192.254.233.89	true	false	0%, Virustotal, Browse	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, 00000003.00000000 2.2114228743.0000000001DA7000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2109091484.000 0000001E17000.00000002.00000000 1.sdmp	false		high
http://www.windows.com/pctv .	rundll32.exe, 00000004.00000000 2.2108934497.0000000001C30000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.00000000 2.2114018629.0000000001BC0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2108934497.000 0000001C30000.00000002.00000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.00000000 2.2114018629.0000000001BC0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2108934497.000 0000001C30000.00000002.00000000 1.sdmp	false		high
http://www.icra.org/vocabulary/ .	rundll32.exe, 00000003.00000000 2.2114228743.0000000001DA7000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2109091484.000 0000001E17000.00000002.00000000 1.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://windowsmedia.com/redirect/services.asp?WMPFriendly=true	rundll32.exe, 00000003.00000000 2.2114228743.0000000001DA7000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2109091484.000 0000001E17000.00000002.00000000 1.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.00000000 2.2114018629.0000000001BC0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2108934497.000 0000001C30000.00000002.00000000 1.sdmp	false		high
http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4	jordji.nbvt11.0.dr	false		high
http://investor.msn.com/	rundll32.exe, 00000003.00000000 2.2114018629.0000000001BC0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2108934497.000 0000001C30000.00000002.00000000 1.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.5.2	anaheimdermatologists.com	United States		46606	UNIFIEDLAYER-AS-1US	false
192.254.233.89	industrialarttextile.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403883
Start date:	04.05.2021
Start time:	13:43:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	statistic-2069354685.xlsm
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:	7
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:	mal84.troj.expl.evad.winXLSM@5/18@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 application associated with file extension: .xlsm - 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, 2.20.142.210, 2.20.142.209, 8.248.113.254, 67.27.157.254, 8.248.131.254, 8.248.115.254, 8.248.137.254 - 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, auto.au.download.windowsupdate.com.c.footprint.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
192.185.5.2	statistic-2070252624.xlsm	Get hash	malicious	Browse	
	statistic-2072807337.xlsm	Get hash	malicious	Browse	
	statistic-207394368.xlsm	Get hash	malicious	Browse	
	statistic-2072807337.xlsm	Get hash	malicious	Browse	
	statistic-207394368.xlsm	Get hash	malicious	Browse	
	catalog-1521295750.xlsm	Get hash	malicious	Browse	
	catalog-1521295750.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	
	f.xlsm	Get hash	malicious	Browse	
	f.xlsm	Get hash	malicious	Browse	
	statistic-118970052.xlsm	Get hash	malicious	Browse	
	statistic-118970052.xlsm	Get hash	malicious	Browse	
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-136896931.xlsm	Get hash	malicious	Browse	
192.254.233.89	statistic-2070252624.xlsm	Get hash	malicious	Browse	
	statistic-2072807337.xlsm	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	statistic-207394368.xlsm	Get hash	malicious	Browse	
	statistic-2072807337.xlsm	Get hash	malicious	Browse	
	statistic-207394368.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	
	statistic-118970052.xlsm	Get hash	malicious	Browse	
	statistic-118970052.xlsm	Get hash	malicious	Browse	
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
industrialarttextile.com	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.254.233.89
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.254.233.89
anaheimdermatologists.com	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.185.5.2
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.185.5.2

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	INDIA ORDERD CH2323ED.exe	Get hash	malicious	Browse	• 162.241.169.22
	ARIX SRLVI (MN) - Italy.exe	Get hash	malicious	Browse	• 192.254.18 5.244
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	GK58.vbs	Get hash	malicious	Browse	• 192.185.21.136
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 50.87.166.59
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 108.179.24 2.122
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 108.179.24 2.122
	6613n246zm543w.xlsm	Get hash	malicious	Browse	• 162.241.24.47
	DEMARG MALAYHCU21345.exe	Get hash	malicious	Browse	• 162.241.169.22
	generated check 662732.xlsm	Get hash	malicious	Browse	• 192.185.177.61
	4Y2I7k0.xlsm	Get hash	malicious	Browse	• 162.241.24.47
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 192.185.13 1.134
UNIFIEDLAYER-AS-1US	statistic-2070252624.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INDIA ORDERD CH2323ED.exe	Get hash	malicious	Browse	162.241.169.22
	ARIX SRLVI (MN) - Italy.exe	Get hash	malicious	Browse	192.254.185.244
	statistic-207394368.xlsm	Get hash	malicious	Browse	192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	192.254.233.89
	presentation.jar	Get hash	malicious	Browse	50.87.249.219
	presentation.jar	Get hash	malicious	Browse	50.87.249.219
	GK58.vbs	Get hash	malicious	Browse	192.185.21.136
	catalog-1521295750.xlsm	Get hash	malicious	Browse	192.185.20.98
	catalog-1521295750.xlsm	Get hash	malicious	Browse	192.185.20.98
	4GGwmv0AJm.exe	Get hash	malicious	Browse	50.87.166.59
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	108.179.242.122
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	108.179.242.122
	6613n246zm543w.xlsb	Get hash	malicious	Browse	162.241.24.47
	DEMARG MALAYHCU21345.exe	Get hash	malicious	Browse	162.241.169.22
	generated check 662732.xlsm	Get hash	malicious	Browse	192.185.177.61
	4Y2I7k0.xlsb	Get hash	malicious	Browse	162.241.24.47
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	192.185.131.134

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	statistic-2070252624.xlsm	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	statistic-2072807337.xlsm	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	statistic-207394368.xlsm	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	e1df57de_by_Libranalysis.xls	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	MV RED SEA.docx	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	SecuriteInfo.com.Heur.31681.xls	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	catalog-1521295750.xlsm	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	471e3984_by_Libranalysis.docx	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	presupuesto.xlsx	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	ORDER INQUIRY.doc	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	Outstanding Payment Plan.xls	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	SecuriteInfo.com.Heur.3421.xls	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	diagram-586750002.xlsm	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	94a5cd81_by_Libranalysis.xls	Get hash	malicious	Browse	192.185.5.2 192.254.233.89
	Documents_585904356_2104184844.xls	Get hash	malicious	Browse	192.185.5.2 192.254.233.89

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Low\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A



Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	7.995478615012125
Encrypted:	true
SSDEEP:	1536:J7r25qSShelms2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwlm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....T.....bR. .authroot.stl...s~.4..CK..8T....c_d....A.K.....&~.J...."Y...\$E.KB..D...D....3.n.u.....].-=H4..c&.....f,=-.-p2...`HX.....b.....Di.a.....M.....4.....i..}:-N.<.>*.V..CX.....B.....q.M.....HB..E~Q...).Gax./.)7..f.....O0...x.k.ha..y.K.0.h.(....{2Y.]g...yw.. 0+?.`-/xvy..e.....w.+^...w .Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.\$Y...u....Z.g.>.0&y.(.<.)>... .R.q...g.Y...s.y.B..B....Z.4.<?.R....1.8.<=.8..[a.s.....add..).NtX.....r....R.&W4.5]....k.._iK..xzW.w.M.>.5.}.).tLX5Ls3_..)!..X.~...%B...YS9m.....BV`.Cee.....?.....x-.q9j...Yps..W...1.A<X.O....7.ei.al.=X...HN.#.....h....y..l.br.8.y"k)....~B..v....GR.g .z..+D8.m..F .h.*.....ltNs\....s.,.f`D...].k...9..lk<D....u.....[...*wY.O...P?.U...l.Fc.ObLq.....Fvk..G9.8..!..T:K'.....'3.....;u..h...uD..^..bS...f.....j..j .=-.s .FxV...g.c.s..9.

C:\Users\user\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:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
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..21093014011520?1\$0"...U...Digital Signature Trust Co.1.0...U...DST Root CA X30..."0...*H.....0.....P..W..be.....k0.[...].@.....3v!*.?!..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...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....r2...D.SrmC.&H.Rg.X..gvqx...V..9\$1....ZOG..P.....dc`.....}...=2.e.. WVv..(9.e...w.j.w.....)...55.1.

C:\Users\user\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):	3.129251112301174
Encrypted:	false
SSDEEP:	6:kKtHmWtJ0N+SkQIPIEGYRM9z+4KIDA3RUe0ht:rhMwTJrkPIE99SNxAhUe0ht
MD5:	4F5E4C2DD3AA32D30BF30638A47A83F9
SHA1:	B6BF02C21B1B0CF38F344597CA3A217AC76AAAFDB
SHA-256:	606F69BE69F8C92D632251DC12D34C2CBDCDCDE29B4762780F4429046BDBCF388C
SHA-512:	9568EF8C3488329B682B2B338D5E6BCEE1981109E6E643006BE27DB3618749C9C3E4DF1A7667ABD5E2A7A9D9EF85BA305D65E7BD57F02B421D3EC3454DA96044
Malicious:	false
Reputation:	low
Preview:	p.....ZgP&A.(.....\$.....http://.ctl.d.l..w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m/.m.s.d.o.w.n.l.o.a.d/.u.p.d.a.t.e/.v.3/.s.t.a.t.i.c./t.r.u.s.t.e.d.r./e.n/.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.8.f.4.f.3.f.6.f.d.7.1.:0."...

C:\Users\user\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data

C:\Users\user\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.0012709523256005
Encrypted:	false
SSDEEP:	3:kkFkITMJYIXfIXIE/jQEBIIPlzRkwWBARLNDU+ZMIKIBkvclcMIVHb1Ffl5n0:kkfYSQE1liBaldQZV7ulPPN
MD5:	22C81A3207323A001185E4D347C8CB62
SHA1:	F9FE61F0813EB67E6894162159F0A8A43832996E
SHA-256:	72A21E4A36B6A07E8B5F3E1F666769E7B8FF00BA80A57FE9B94AC430DA47F88D
SHA-512:	4B43ECE113A0CA88BDD47D14F5597140377CA48265C2FDD57E63EB764083E58B46359D9C85D5089A599850706F94036DF56E886E9DD5C364ADDB7C0E8A32196
Malicious:	false
Reputation:	low
Preview:	p.....`....w)P&A..(..... j-.....(.....)....h.t.t.p://.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..."3.7.d.-.5.b.f.8.d.f.8.0.6.2.7.0.0"...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\suspendedpage[1].htm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	494
Entropy (8bit):	4.962239405540505
Encrypted:	false
SSDEEP:	12:hnmQbwzRQ6QclfhxxEdWr+YZrH3atJMIgOt0quoQL:hMxRQspxCQnZrH3atEx0h
MD5:	0357AA49EA850B11B99D09A2479C321B
SHA1:	41472BA5C40F61FA1C77C42CF06248F13B8785F0
SHA-256:	0FF0B7FCB090C65D0BDCB2AF4BBD2C30F33356B3CE9B117186FA20391EF840A3
SHA-512:	A317A0F035B8DFF7CA60C76B0B75698A3528FD4C7C5E915292C982D2B38C1C937C318362C891E93BEE6FDB1B166764D7183140A837FD23DAA2BE3D2DAC5A5DC
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://anaheimdermatologists.com/cgi-sys/suspendedpage.cgi
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>.<head>.<title>Contact Support</title>.<meta http-equiv="Content-Type" content="text/html; charset=utf-8">.</head>.<body marginwidth="0" marginheight="0" leftmargin="0" topmargin="0">.<iframe width="100%" height="100%" frameborder="0" SCROLLING="auto" marginwidth="0" src="http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4"></iframe>.</body>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\216A9434.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 205 x 58, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8301
Entropy (8bit):	7.970711494690041
Encrypted:	false
SSDEEP:	192:BzNWXTPmjktA8BddiGGwjNHOQRud4JTTOFPY4:B8aoVT0QNuzWKPh
MD5:	D8574C9CC4123EF67C8B600850BE52EE
SHA1:	5547AC473B3523BA2410E04B75E37B1944EE0CCC
SHA-256:	ADD8156BAA01E6A9DE10132E57A2E4659B1A8027A8850B8937E57D56A4FC204B
SHA-512:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBACF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....!J.....sRGB.....pHYs.....+.....IDATx^.\....}.16"Sp...g.9Ks..r.=r.U....Y..l.S.2...Q.`C.....h}x.....\..N...z....._]......Ill.666...~::~.6l.Q.J...\.m.g.h.SRR.\p....'N...EEE...X9.....c.&M...].n.g4..E.g...w...{.];w..l..y.ml...~...;].3{~.qV.k.....?..w/\$Gll .2. m,,,-[.....sr.V1.g...on.....dl.'...'[[[R.....(.^...F.PT.Xq..Mnnn.3..Ml.g.....6....pP"#F..P/S.L...W.^..o.r....5H.....111t...[9.3...J..>...[.t-/F.b..h.P..jz...o..4n.F..e..0!!!!.....#"h.K.K....g.....^..w!.\$.&...7n.J.F.\A...6lxjj.K/.....g.....3g...f...t..s..5.C4..+W.y...88..?.Y..^..8{. @VN.6....Kbch.=zt..7+T...v.Z...P.....VVV..."tN.....\$.Jag.v.U...P[(_l?9.4i.G.\$U.D.....W.f.....!> . #G...3..x.b.....P...H!Vj.....u.2.*;..Z..c..._Ga...&L.....`.1.[.n].7..W_m...#8k...)U..L....G..q.F.e>..s.....q....J....(N.V...k..>m....=).

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7417EC62.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5I9TvSb5LrU7+uHK2yJtNJTNSB0qNMQCvGEvfqVfSsq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7417EC62.png	
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l9a_.X....@.`ddbc.].....O..m7.r0]..."?A.....w.;N1u....._[.lY...BK=...F+t.M~..oX..%....211o.q.P.".....y..../.l.r...4..Q].h.....LL.d.....d...w.>{e..k.7.9y.%..Ypl..{+Kv...../.[.A....^5c..O?.....G...VB..4HWY...9NU...?.S.\$..1..6.U.....c... ..7..J. "M..5.d.V.W.c.....Y.A..S....~.C.....q.....t?..."n....4.....G.....Q..x.W.l.A...3...MR.-.P#p;.p_.....jUG...X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\82F80CFB.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:Jljm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F86421206467f
Malicious:	false
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q...;3...?.fk.IR..R\$.Pb.Q...B..OA..T\$.hAD...J./.-h..fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;s...O.....;y.p.....s1@ l.r....>.LLa..b?h...l.6..U....1...r....T..O.d.KSA...7.YS..a.(F@...xe.^..l.\$h..PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k..d.&..Xa.t.E...E..f2.d(..v..~.P..+pik+;...xEU.g....._xfw...+...(.pQ.(.(U./..).@..?.....f'...lx+@F...+....).k.A2...r~B,...TZ..y..9...`..0....q....yY....Q.....A...8j[.O9..t.&...g. l@ ..;..Xl...9S.J5..'.xh...8l..~..+...mf.m.W.i.{...+>P...Rh...+.br^\$. q.^.....(....j...\$.Ar...MZm]...9..E..!Uj.S.fDx7<...Wd.....p..C.....^Myl:...c.^..Sl.mGj.....!...h..\$.;.....yD/..a...j.^..}.v....RQY*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A28A3EA5.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 485 x 185, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	34787
Entropy (8bit):	7.9883689087667955
Encrypted:	false
SSDEEP:	768:XbyxVN2hP86XpVBxUmtCQHcQpKvtcFM/MoJ97bk3Ueu:m92hjPcQpWUot9Eg
MD5:	2C5A59B7F30E5E41412EC22FDEA1DBB5
SHA1:	9A64FB6A68683EEC580A881725DBD146E80D06B1
SHA-256:	E872E66F60AE5651AE96A2C2A88D07B0D1C96CDDD45F787AB04237891AD4E8FB
SHA-512:	2D494F44E1DA36794C3E707BF1173EE63E2CF3101E3B5EA60D71A194DA9A6A1EB6B9C166B7C1ACAA2D455B9C6413D0FEE40AD38972C076183EF167818D7E92fC
Malicious:	false
Preview:	.PNG.....IHDR.....i.....sRGB.....pHYs.....+.....IDATx^...JU>..{.....".bA.6.6..o/3.....b...{HBBz./.....[. %yl!>...}.^{o.....^..R.....=.c..-Z.n]cc...W.^.....z...2.9s.<....?_j&....R.....K...\.V..ukS.sgKKKWWWkk_@s....<x.Q.t.1bt.5k.QG....X0f..Y.T.....k..y..k..K6^...v.x}.p...vX.MK..5....j...X...8...~.....z.{aJ.Q...{._]...{ui..M.)^..l.....};>..{n...../^..hnn.t.^)..S.Ly.3.q.W.v.i)d....W.x=p".d@k.(y...kE..P.....mH"F^...\q.v)....K...R...:O..i..G.....?..!.....y.^..W.....u...).c.j _=...X.....<..u.]w.7.H..;GE*...x.;^..WM.8.....G..x.?.*.....F..~..k.f.%kN {..}(d..C.z...2.G....x...S*^.....c.?..o..ME`.....s.9.{.....>;5....o.T.....l.....?..o.w.6./~..>...S.i1.Q).^..Vle.....~.._./..G...!C..... .k]]v.x.wt.....=.Y0.Z..9.....=t....][S.)^Mm...p..m.....M.6...r.L.6MT..3'M.4{I~P[h....Wtttx.....#.OR.l.r.e@

C:\Users\user\AppData\Local\Temp\0CDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	109076
Entropy (8bit):	7.917022545802549
Encrypted:	false
SSDEEP:	1536:oeuov3BiTr4GDgM+1M92hjPcQpWUot9ENPcNcrAOJOerwzKFbHhr6vQnf+zyyfqk:oeuocrZD2MopH8x+FHdLqp6vif+zbj
MD5:	74AE1B685F40E9853B1CDBF7545042DA
SHA1:	C45DE5DECD85C1A40A35818310731B49AB3F8B74
SHA-256:	3F18EA5A430438B03923B8E0511D08D9D0A657720BC64E07D614038A0D9CD905
SHA-512:	E186D43D0FA831280FAE21B79B391912F58ABF0F51CA31F1269A9710A80B3395D179E7E34267D0A5B9328CF7BE959DE1FDDE147879B3664E46136B08D1FE1D68
Malicious:	false
Preview:	.U.n.0...?.....C....l?&..a..e.....5..Jr.....jcM....w-.hf..'k....0.....Z..dW.....XQ...)... .G3+..H.;..l..l..K...T.....&U....)Yj....2U.D.FK.H(r..... ...`....&DM...R....u...f.y.xE...%#2.....^..~.^a.3..0.....ZAu'b.....}V_7.A...k.HOMq..BF.....^..~.*.....7.....E..V.-f....2.n:h.]]a..J..l...c.....~..c.E.u.(...../.....s.....>.....>.q...\$Y....AL..Yv.)......a.@....pZ.....PK.....!t.....[Content_Types].xml ...(.....

C:\Users\user\AppData\Local\Temp\CabE725.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	7.995478615012125
Encrypted:	true
SSDEEP:	1536:J7r25qSShelms2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwlm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....l.....T.....bR. .authroot.stl...s~.4..CK..8T....c_d....A.K.....&-J...."Y...\$E.KB..D...D.....3.n.u..... .]=H4.c&.....f,=-.-...p2...`HX.....b.....Di.a.....M.....4.....i..}:-N<.>*.V..CX.....B.....q.M.....HB..E~Q...).Gax./..}7..f.....O0...x.k.ha..y.K.0.h.(....{2Y.]g...yw.. 0.+?.`-/xvy.e.....w.+^..w Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....P.\$Y...u....Z..g.>.0&y.(.<.]>... .R.q..g.Y..s.y.B...Z.4.<?.R...1.8.<=.8.[a.s.....add..).NtX....r....R.&W4.5]...k.._iK..xzW.w.M.>.5.}.).tLX5Ls3_..)!X~...%B....Y\$9m.....BV`.Cee.....?.....:x-.q9j...Yps.W...1.A<X.O...7.ei.al~=-X...HN.#....h...y..l.br.8.y"k)....~B..v....GR.gl.z..+D8.m..F .h..*.....ltNs\....s...f`D...].k...9...lk<D....u.....[...*.wY.O...P?.U.l...Fc.Oblq.....Fvk..G9.8..!..t:K`.....'3.....;u..h...uD...^..bS...f.....j..j .=-..s..FxFV...g.c.s..9.

C:\Users\user\AppData\Local\Temp\TarE726.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.309740459389463
Encrypted:	false
SSDEEP:	1536:Tlz6c7xcjgCyrYBZ5pimp4Ydm6Caku2Dnsz0JD8reJgMnl3rlMGgv:TNqccCymfdmoku2DMykMnNGG0
MD5:	4E0487E929ADBBA279FD752E7FB9A5C4
SHA1:	2497E03F42D2CBB4F4989E87E541B5BB27643536
SHA-256:	AE781E4F9625949F7B8A9445B8901958ADECE7E3B95AF344E2FCB24FE989EEB7
SHA-512:	787CBC262570A4A23FD9C2BA6DA7B0D17609C67C3FD568246F9BEF2A138FA4EBCE2D76D7FD06C3C342B11D6D9BCD875D88C3DC450AE41441B6085B2E5D485A
Malicious:	false
Preview:	0..T...*H.....T.O..T.....1.0...`H.e.....0..D...+.....7...D.O..D.O...+.....7..... h.....210303062855Z0...+.....0..D.O.*.....`...@...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". .jL4.>.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..%i...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.O.D...+.....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...JlU".F....9.N...`...00...+.....7..b1". .@.....G.d.d.m.\$...X...)0B..+.....7...14.2M.i.c.r.o.s.o.f.t..R.o.o.t..A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Tue May 4 19:44:41 2021, atime=Tue May 4 19:44:41 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.484398415815576
Encrypted:	false
SSDEEP:	12:85QAnyKk0LgXg/XAICPCHaXtB8XzB/GLf/xX+WnicvbwbDtZ3YilMMEpxRljKlcs:85/yI/XTd6jw/xYegDv3qfrNru/
MD5:	DD0604BCE70E45479C53C63FC04CAD71
SHA1:	8A1B7D31F07A2960A5690ABE07E6852DE5D8D7DB
SHA-256:	EE0A698FFCE0C54CDE21B7309704F3C5BF602FE2EBA2B74FC0DC1925167270CE
SHA-512:	8BE8DC629347C363EC3CA20E7E4718821CDA17DC1739D733E587CB8130EA5813247FD15D2549437D0050D18FDE15B6B1A27204036E5B22204F34577491631930
Malicious:	false
Preview:	L.....F.....7G....N&A....N&A.....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\..#.....\305090\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.-3.6.7.3.6.4.7.7.-1.0.0.6.....`.....X.....305090.....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):	115
Entropy (8bit):	4.59911576030832
Encrypted:	false
SSDEEP:	3:oyBVomxWdacEI2OytcEI2mxWdacEI2v:djuaZtZaj

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
MD5:	19FC1324EF0021D509D5A8DAF316C4DF
SHA1:	60FF2DF708BD84B80D40E01FF037C9D61F478E46
SHA-256:	68782E3476F3DA67AB4D1796164708A27E2CE02134A59429591A41C6C7964DA8
SHA-512:	1DC19FAC86C265AE967CDEBC8EFA5464794FC8D1246E50652D2A504DB3D419B7F6D1AD701F481B296A0C3D86DC3CF92DF15A73DEF230DCBA7E7D629D4533611
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..statistic-2069354685.LNK=0..statistic-2069354685.LNK=0..[misc]..statistic-2069354685.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\statistic-2069354685.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 Aug 26 14:08:16 2020, mtime=Tue May 4 19:44:41 2021, atime=Tue May 4 19:44:41 2021, length=109076, window=hide
Category:	dropped
Size (bytes):	2138
Entropy (8bit):	4.551928545797767
Encrypted:	false
SSDEEP:	48:8ZK/XTOjFpfJhxO6YfQh2ZK/XTOjFpfJhxO6YfQ/8a/XojFpfZO6YfQh2a/XojFpfZO6YfQ/
MD5:	7F3A420A1FB1AEDA14809CFF6E3275D8
SHA1:	89B87D890C8B5DB508E457AFDF5B70A2C263FBBA
SHA-256:	8B1370F81A11AD27F3A5F2E06D5C25A5C27E0DD526AD991182229867E9B58957
SHA-512:	F6196307AF28F687E232DECA64066164AD6B8E60D7A33C57D8039C28EF8126795E6DBF9310F954F9448A42E4660E95740EDFD65AB4BCBD4B86AAD9F82F330518
Malicious:	false
Preview:	L.....F.....B{...N&A.....N&A.....P.O.+00.../C\.....t.1.....QK.X\Users\.....QK.X*.....6.....User.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.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....j.2.....R..STATIS-1.XLS.'.....Q.y.Q.y*...8.....s.t.a.t.i.s.t.i.c.-2.0.6.9.3.5.4.6.8.5...x.l.s.m.....-8...[.....?J.....C:\Users\..#.....\305090\Users.user\Desktop\statistic-2069354685.xlsm.0.....\.....\D.e.s.k.t.o.p.\s.t.a.t.i.s.t.i.c.-2.0.6.9.3.5.4.6.8.5...x.l.s.m.....(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.....305090.....

C:\Users\luser\Desktop\0DDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	109076
Entropy (8bit):	7.917022545802549
Encrypted:	false
SSDEEP:	1536:oeuov3BiTr4GDgM+1M92hjPcQpWUot9ENPcNcrAOJOerwzkFBHhr6vQnf+zyyfqk:oeuocrZD2MopH8x+FHdoLqp6vif+zbj
MD5:	74AE1B685F40E9853B1CDBF7545042DA
SHA1:	C45DE5DECD85C1A40A35818310731B49AB3F8B74
SHA-256:	3F18EA54A30438B03923B8E0511D08D9D0A657720BC64E07D614038A0D9CD905
SHA-512:	E186D43D0FA831280FAE21B79B3919212F58ABF0F51CA31F1269A9710A80B3395D179E7E34267D0A5B9328CF7BE959DE1FDDE147879B3664E46136B08D1FE1D68
Malicious:	false
Preview:	.U.n.0...?.....C...l?&.a.e....5..Jr.....jcM...w-hf.'k....0....Z.dW.....XQ...). .G3+...H...;\...l.K...T.....&U....)Yj....2U.D.FK.H(r..... ...`....&DM...R....u...f.y xE...%#2....`-!^a.3.0....ZAU'b.....)V_7.A...k.H0Mq..BF.....^.'*.....7.....E..V-f....2.n:h.]]a.J.../..c.....-c.E.u(...../.....s.....>.....>..q...\$Y...AL.Yv,).....a.@ ...pZ.....PK.....!t.....[Content_Types].xml ...(.....

C:\Users\user\Desktop\~\$statistic-2069354685.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fv:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	true
Preview:	<pre> .user ..A.I.b.u.s.user ..A.I.b.u.s. </pre>

C:\Users\userljordji.nbvt11	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	494
Entropy (8bit):	4.962239405540505
Encrypted:	false
SSDEEP:	12:hnMQbwzRQ6QclfhxxEdWr+YZrH3atJMIgOt0quoQL:hMxRQspxCQnZrH3atEx0h
MD5:	0357AA49EA850B11B99D09A2479C321B
SHA1:	41472BA5C40F61FA1C77C42CF06248F13B8785F0
SHA-256:	0FF0B7FCB090C65D0BDCB2AF4BBD2C30F33356B3CE9B117186FA20391EF840A3
SHA-512:	A317A0F035B8DFF7CA60C76B0B75698A3528FD4C7C5E915292C982D2B38C1C937C318362C891E93BEE6FDB1B166764D7183140A837FD23DAA2BE3D2DAC5A5DC
Malicious:	false
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>.<head>.<title>Contact Support</title>.<meta http-equiv="Content-Type" content="text/html; charset=utf-8">.</head>.<body marginwidth="0" marginheight="0" leftmargin="0" topmargin="0">.<iframe width="100%" height="100%" frameborder="0" SCROLLING="auto" marginwidth="0" src="http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4"></iframe>.</body>.</html>.

Static File Info

General	
File type:	Microsoft Excel 2007+
Entropy (8bit):	7.917058358399405
TrID:	- Excel Microsoft Office Open XML Format document (40004/1) 83.33% - ZIP compressed archive (8000/1) 16.67%
File name:	statistic-2069354685.xlsm
File size:	109084
MD5:	e594ea809c24d81cacae25761ae68a4d
SHA1:	c402e78a57d801ee6220aa1e8532e444db22f911
SHA256:	d328633005bb0fd39826107193a26f4d6d933fb4f2dfb6f8e4eb48c6eab81df3
SHA512:	01e3c852814d23f57b206ff2f6b4f0c0f55cf76ed7bc77483688e2a86d2c4b4112487b1e157b25adf81ac0b64afd144fae8c720e1c1c39bd9bd8d06dd06fd4e2
SSDEEP:	1536:cutuov3BiTr4GDgM+nG92hjPcQpWUot9E8cNcrAOJOerwzkFBHr6vQnf+zy7fc:ckuocrZDKGopH8x+8HdoLqp6vif+zuK
File Content Preview:	PK.....!t.....[Content_Types].xml ...(.....

File Icon

	
Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General	
Document Type:	OpenXML
Number of OLE Files:	1

OLE File "statistic-2069354685.xlsm"

Indicators	
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	

Indicators	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Flash Objects Count:

Macro 4.0 Code

[illegible]

.....=HALT(0),....."=4984654+9846544+468464=CALL(Sheet2!AY107&"n",Sheet2!AY108&"A",Sheet2!AY118.before.3.21.42.sheet!AR49,Sheet2!AT114.before.3.21.42.sheet!AT39,0,0)=CALL(Sheet2!AY107&"n",Sheet2!AY108&"A",Sheet2!AY118.before.3.21.42.sheet!AR49,Sheet2!AT115.before.3.21.42.sheet!AT39&"1","0"),.....=Sheet2!AW142(.....,U,J,"D"...j0rdji.nbvt1R,J,L,C,I,D

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:44:22.960942984 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:44:23.145898104 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:44:23.146073103 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:44:23.157212973 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:44:23.344053984 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:44:23.354043007 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:44:23.354080915 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:44:23.354103088 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:44:23.354195118 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:44:23.407183886 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:44:23.598262072 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:44:23.598474026 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:44:25.226177931 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:44:25.451641083 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:44:25.770373106 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:44:25.770546913 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:44:25.770726919 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:44:25.770812035 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:44:25.771151066 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:44:25.846358061 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:25.957715988 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:44:26.011251926 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:44:26.011380911 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:26.012357950 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:26.177603960 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:44:26.268949986 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:44:26.268986940 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:44:26.269005060 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:44:26.269207001 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:26.318813086 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:26.482270956 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:44:26.494283915 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:44:26.494405985 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:26.527581930 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:26.706720114 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:44:26.706753016 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:44:26.706955910 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:26.707367897 CEST	49170	443	192.168.2.22	192.185.5.2

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:44:26.709048033 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:26.871176004 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:44:26.874960899 CEST	443	49171	192.185.5.2	192.168.2.22
May 4, 2021 13:44:26.875137091 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:26.875727892 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:27.038769007 CEST	443	49171	192.185.5.2	192.168.2.22
May 4, 2021 13:44:27.043895006 CEST	443	49171	192.185.5.2	192.168.2.22
May 4, 2021 13:44:27.044063091 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:27.044629097 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:27.076562881 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:27.239655018 CEST	443	49171	192.185.5.2	192.168.2.22
May 4, 2021 13:44:27.411127090 CEST	443	49171	192.185.5.2	192.168.2.22
May 4, 2021 13:44:27.411268950 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:27.411535978 CEST	443	49171	192.185.5.2	192.168.2.22
May 4, 2021 13:44:27.411624908 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:27.412714005 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:44:27.575457096 CEST	443	49171	192.185.5.2	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:44:22.742083073 CEST	52197	53	192.168.2.22	8.8.8.8
May 4, 2021 13:44:22.942532063 CEST	53	52197	8.8.8.8	192.168.2.22
May 4, 2021 13:44:23.972698927 CEST	53099	53	192.168.2.22	8.8.8.8
May 4, 2021 13:44:24.027863979 CEST	53	53099	8.8.8.8	192.168.2.22
May 4, 2021 13:44:24.034517050 CEST	52838	53	192.168.2.22	8.8.8.8
May 4, 2021 13:44:24.085961103 CEST	53	52838	8.8.8.8	192.168.2.22
May 4, 2021 13:44:24.633137941 CEST	61200	53	192.168.2.22	8.8.8.8
May 4, 2021 13:44:24.692380905 CEST	53	61200	8.8.8.8	192.168.2.22
May 4, 2021 13:44:24.700788975 CEST	49548	53	192.168.2.22	8.8.8.8
May 4, 2021 13:44:24.761848927 CEST	53	49548	8.8.8.8	192.168.2.22
May 4, 2021 13:44:25.785185099 CEST	55627	53	192.168.2.22	8.8.8.8
May 4, 2021 13:44:25.844109058 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 4, 2021 13:44:22.742083073 CEST	192.168.2.22	8.8.8.8	0xccae	Standard query (0)	industrialarttextile.com	A (IP address)	IN (0x0001)
May 4, 2021 13:44:25.785185099 CEST	192.168.2.22	8.8.8.8	0x9ffe	Standard query (0)	anaheimdermatologists.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 13:44:22.942532063 CEST	8.8.8.8	192.168.2.22	0xccae	No error (0)	industrialarttextile.com		192.254.233.89	A (IP address)	IN (0x0001)
May 4, 2021 13:44:25.844109058 CEST	8.8.8.8	192.168.2.22	0x9ffe	No error (0)	anaheimdermatologists.com		192.185.5.2	A (IP address)	IN (0x0001)

HTTPS Packets

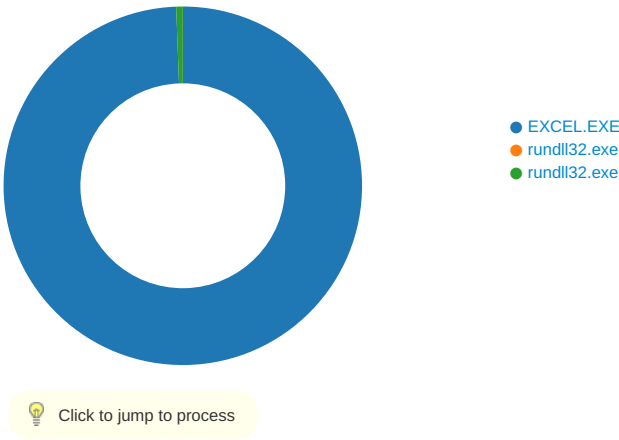
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 13:44:23.354103088 CEST	192.254.233.89	443	192.168.2.22	49167	CN=mail.gdmart.com.bd CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Mar 10 10:47:11 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 08 11:47:11 CEST 2021 Wed Sep 29 21:21:40 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		
May 4, 2021 13:44:26.269005060 CEST	192.185.5.2	443	192.168.2.22	49170	CN=cpcalendars.anaheimdermatologists.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.	Wed Mar 17 22:18:32 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 15 23:18:32 CEST 2021 Wed Sep 29 21:21:40 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		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2116 Parent PID: 584

General

Start time:	13:44:38
Start date:	04/05/2021
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:	0x13ffa0000
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\D9EB.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	1402EEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\0CDE0000	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~\$statistic-2069354685.xlsm	read attributes delete syn chronize generic read generic write	device	synchronous io non alert non directory file delete on close open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DDE0000	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FEEAC59AC0	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	140CC828C	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	140CC828C	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	140CC828C	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	140CC828C	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	140CC828C	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	140CC828C	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	140CC828C	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	140CC828C	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	140CC828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\jordi.nbvt11	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	140CC828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\2CBE.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	1402EEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ID9EB.tmp	success or wait	1	14055B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\limg_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image003.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image015.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image016.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image017.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image018.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image019.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\filelist.xml~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\2CBE.tmp	success or wait	1	14055B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0CDE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\0DD00000	C:\Users\user\Desktop\statistic-2069354685.xlsm	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\limg_files\stylesheet.cs~..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\limg_files\tabstrip.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\limg_files\sheet001.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image003.png	C:\Users\user\AppData\Local\Temp\limg_files\image003.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image015.png	C:\Users\user\AppData\Local\Temp\limg_files\image015.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image016.png	C:\Users\user\AppData\Local\Temp\limg_files\image016.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image017.png	C:\Users\user\AppData\Local\Temp\limg_files\image017.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image018.png	C:\Users\user\AppData\Local\Temp\limg_files\image018.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image019.png	C:\Users\user\AppData\Local\Temp\limg_files\image019.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\filelist.xml	C:\Users\user\AppData\Local\Temp\limg_files\filelist.xml~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\limg_files\stylesheet.css..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\limg_files\tabstrip.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\limg_files\sheet001.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image020.pn_	C:\Users\user\AppData\Local\Temp\limg_files\image020.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image021.pn_	C:\Users\user\AppData\Local\Temp\limg_files\image021.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image022.pn_	C:\Users\user\AppData\Local\Temp\limg_files\image022.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image023.pn_	C:\Users\user\AppData\Local\Temp\limg_files\image023.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image024.pn_	C:\Users\user\AppData\Local\Temp\limg_files\image024.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\image025.pn_	C:\Users\user\AppData\Local\Temp\limg_files\image025.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\limg_files\filelist.xml_	C:\Users\user\AppData\Local\Temp\limg_files\filelist.xmlss	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~\$statistic-2069354685.xlsm	unknown	55	05 41 6c 62 75 73 20	.user	success or wait	1	1401EF526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0CDE0000	107274	1802	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 74 c0 ce fe c4 01 00 00 dd 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 fd 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 ba 36 91 b4 34 01 00 00 56 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 23 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 f1 ff 6c b6 11 02 00 00 da 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 97 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!t.....[Content_Types].xmlPK..-.....!..U0#...L_rels/.re !sPK..-.....!..6..4...V...#...xl/_rels/wor kbook.xml.relsPK..-.....! ..!..... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~\$statistic-2069354685.xlsm	unknown	55	05 41 6c 62 75 73 20	.user	success or wait	1	1401EF526	WriteFile
C:\Users\user\Desktop\~\$statistic-2069354685.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	1401EF591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\suspendedpage[1].htm	unknown	494	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 43 6f 6e 74 61 63 74 20 53 75 70 70 6f 72 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 20 20 20 3c 62 6f 64 79 20 6d 61 72 67 69 6e 77 69 64 74 68 3d 22	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Suppo rt</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="	success or wait	1	140CC828C	URLDownloadToFileA
C:\Users\user\jordi.nbvt11	unknown	494	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 43 6f 6e 74 61 63 74 20 53 75 70 70 6f 72 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 20 20 20 3c 62 6f 64 79 20 6d 61 72 67 69 6e 77 69 64 74 68 3d 22	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Suppo rt</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="	success or wait	1	140CC828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\82F80CFB.png	0	848	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A28A3EA5.png	0	34787	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\216A9434.png	0	8301	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7417EC62.png	0	557	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\statistic-2069354685.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\statistic-2069354685.xlsm	0	8	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\216A9434.png	0	8301	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A28A3EA5.png	0	34787	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7417EC62.png	0	557	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\82F80CFB.png	0	848	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\216A9434.png	0	8301	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A28A3EA5.png	0	34787	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7417EC62.png	0	557	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\82F80CFB.png	0	848	success or wait	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	6	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	6	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDA29	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDB04	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDBAF	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDCB8	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDD93	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\103727	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\104470	success or wait	1	7FEEAC59AC0	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	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	4	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	4	7FEEAC59AC0	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	2	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown

[illegible]

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

Analysis Process: rundll32.exe PID: 2652 Parent PID: 2116

General

Start time:	13:44:46
Start date:	04/05/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..jordji.nbvt1,DllRegisterServer
Imagebase:	0xffe30000
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: 2552 Parent PID: 2116

General

Start time:	13:44:47
Start date:	04/05/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..jordji.nbvt11,DllRegisterServer
Imagebase:	0xffe30000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\jordji.nbvt11	unknown	64	success or wait	1	FFE327D0	ReadFile

Disassembly

Code Analysis