

JOeSandbox Cloud BASIC



ID: 355906

Sample Name: document-1019153116.xls

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 09:07:46

Date: 22/02/2021

Version: 31.0.0 Emerald

Table of Contents

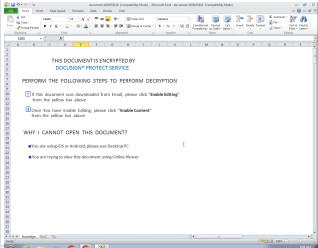
Table of Contents	2
Analysis Report document-1019153116.xls	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Initial Sample	4
Sigma Overview	4
System Summary:	5
Signature Overview	5
AV Detection:	5
Compliance:	5
Software Vulnerabilities:	5
System Summary:	5
HIPS / PFW / Operating System Protection Evasion:	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	8
Domains and IPs	8
Contacted Domains	8
URLs from Memory and Binaries	8
Contacted IPs	8
Public	9
General Information	9
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	11
Static File Info	12
General	12
File Icon	13
Static OLE Info	13
General	13
OLE File "document-1019153116.xls"	13
Indicators	13
Summary	13
Document Summary	13
Streams	13
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096	13
General	13
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096	14
General	14

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 80660	14
General	14
Macro 4.0 Code	14
Network Behavior	14
Network Port Distribution	14
TCP Packets	15
UDP Packets	15
DNS Queries	15
DNS Answers	15
Code Manipulations	16
Statistics	16
Behavior	16
System Behavior	16
Analysis Process: EXCEL.EXE PID: 2268 Parent PID: 584	16
General	16
File Activities	16
File Created	16
File Deleted	17
File Moved	17
File Written	18
File Read	25
Registry Activities	25
Key Created	25
Key Value Created	25
Analysis Process: rundll32.exe PID: 2028 Parent PID: 2268	33
General	33
File Activities	34
Disassembly	34
Code Analysis	34

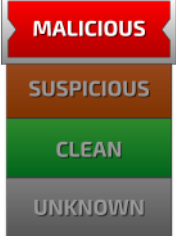
Analysis Report document-1019153116.xls

Overview

General Information

Sample Name:	document-1019153116.xls
Analysis ID:	355906
MD5:	948a7b1bc28afb2.
SHA1:	8f858737a636e73.
SHA256:	4e657cfccf1d18b...
Tags:	SilentBuilder xls
Most interesting Screenshot:	
	

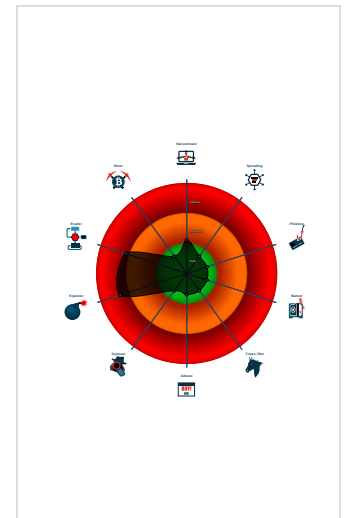
Detection

	
Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm...
Office document tries to convince vi...
Document exploit detected (UrlDown...
Document exploit detected (process...
Found Excel 4.0 Macro with suspicio...
Sigma detected: Microsoft Office Pr...
Yara detected hidden Macro 4.0 in E...
Document contains embedded VBA ...
Potential document exploit detected...
Potential document exploit detected...
Potential document exploit detected...
Yara signature match

Classification



Startup

- System is w7x64
-  EXCEL.EXE (PID: 2268 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
 -  rundll32.exe (PID: 2028 cmdline: rundll32 ..\iopjvdf.vock,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
document-1019153116.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	0x11c58:\$e1: Enable Editing 0x11ccd:\$e2: Enable Content
document-1019153116.xls	SUSP_Excel4Macro_Auto Open	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	0x0:\$header_docf: D0 CF 11 E0 0x13ea2:\$s1: Excel 0x14efd:\$s1: Excel 0x36b7:\$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1019153116.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

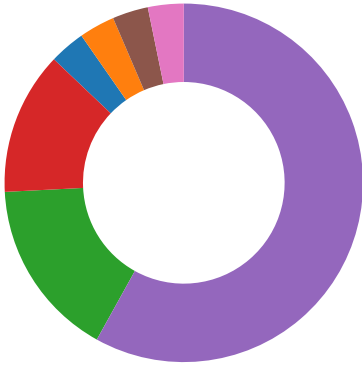
Sigma Overview

System Summary:



Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Compliance:



Uses new MSVCR DLLs

Software Vulnerabilities:



Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:



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

HIPS / PFW / Operating System Protection Evasion:



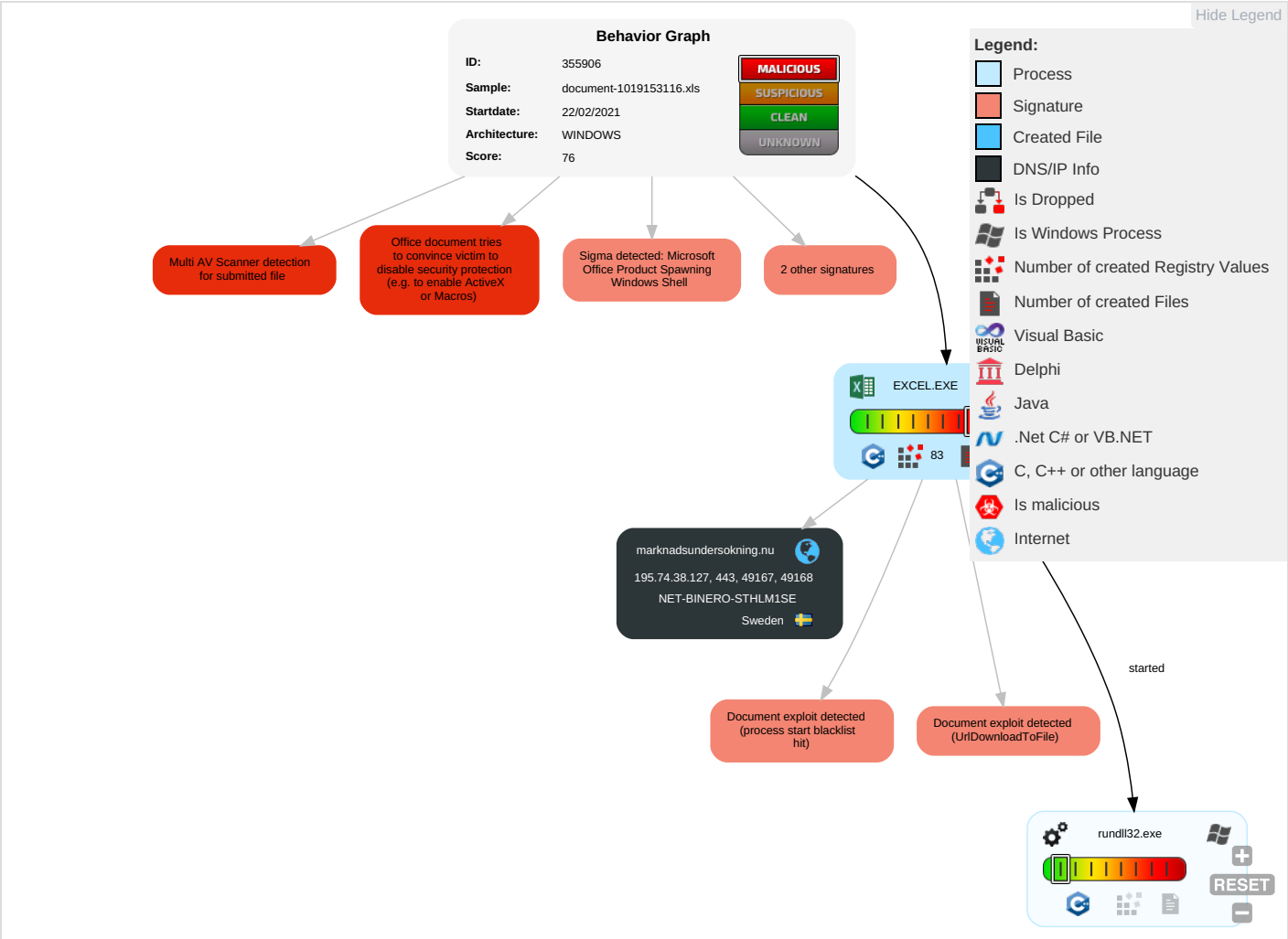
Yara detected hidden Macro 4.0 in Excel

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 1 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	Malicious Software

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
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	Di
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	Di Di Di
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		Ci Bi Fr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R or

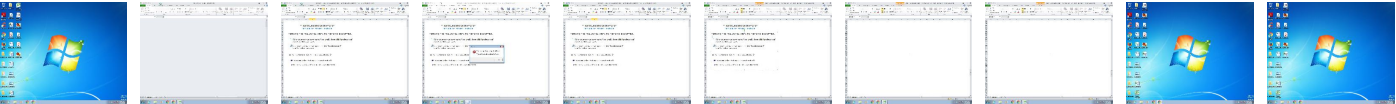
Behavior Graph

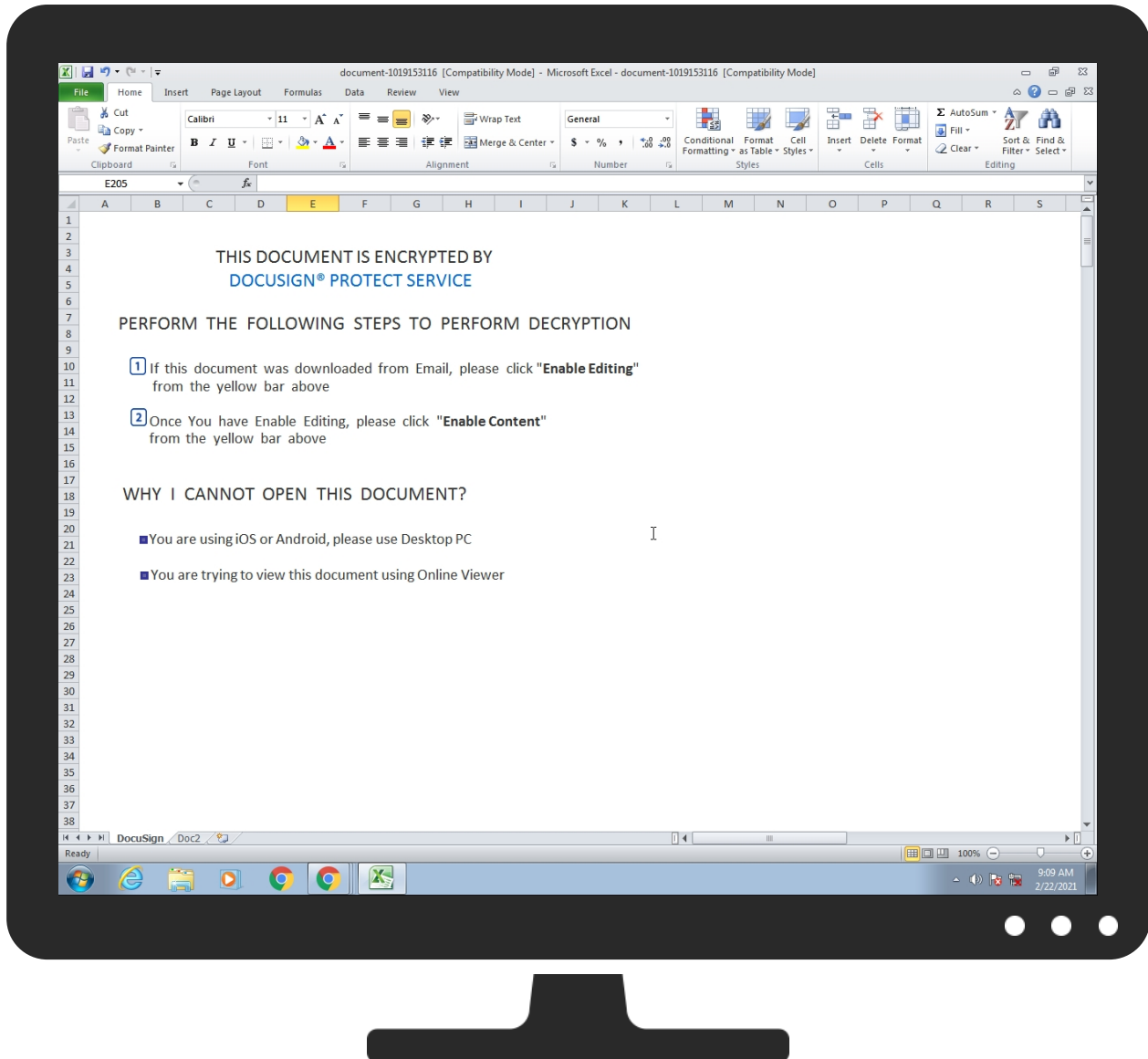
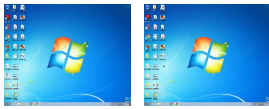


Screenshots

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
document-1019153116.xls	21%	ReversingLabs	Document-Word.Backdoor.Quakbot	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
marknadsundersokning.nu	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/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://marknadsundersokning.nu/ds/1902.gif	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
marknadsundersokning.nu	195.74.38.127	true	false	0%, Virensafe, 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, 00000003.00000000.2.2099351808.0000000001E27000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv	rundll32.exe, 00000003.00000000.2.2099153587.0000000001C40000.00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.00000000.2.2099153587.0000000001C40000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.00000000.2.2099153587.0000000001C40000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/	rundll32.exe, 00000003.00000000.2.2099351808.0000000001E27000.00000002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.00000000.2.2099351808.0000000001E27000.00000002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.00000000.2.2099153587.0000000001C40000.00000002.00000001.sdmp	false		high
http://https://marknadsundersokning.nu/ds/1902.gif	document-1019153116.xls	false	Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000003.00000000.2.2099153587.0000000001C40000.00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.74.38.127	unknown	Sweden		35041	NET-BINERO-STHLM1SE	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355906
Start date:	22.02.2021
Start time:	09:07:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1019153116.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	- HCA enabled - EGA enabled - HDC enabled - AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.expl.evad.winXLS@3/5@1/1
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: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.74.38.127	document-1109482545.xls	Get hash	malicious	Browse	
	document-1109482545.xls	Get hash	malicious	Browse	
	http://https://danborjesson.com/main.php/#jeanserge_hien@iamgold.com	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
marknadsundersokning.nu	document-1109482545.xls	Get hash	malicious	Browse	• 195.74.38.127
	document-1109482545.xls	Get hash	malicious	Browse	• 195.74.38.127

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NET-BINERO-STHLM1SE	document-1109482545.xls	Get hash	malicious	Browse	• 195.74.38.127
	document-1109482545.xls	Get hash	malicious	Browse	• 195.74.38.127
	7BkDeaSmzd.doc	Get hash	malicious	Browse	• 195.74.38.63
	ins.exe	Get hash	malicious	Browse	• 195.74.38.62
	inv.exe	Get hash	malicious	Browse	• 195.74.38.62
	New Purchase Order 501,689\$.exe	Get hash	malicious	Browse	• 195.74.38.62
	New Purchase Order 50,689\$.exe	Get hash	malicious	Browse	• 195.74.38.62
	nko-Fichero-ES.msi	Get hash	malicious	Browse	• 195.74.38.93
	dy-Fichero-ES.msi	Get hash	malicious	Browse	• 195.74.38.93
	oym-FicheroES.msi	Get hash	malicious	Browse	• 195.74.38.93
	http://ctannous.com/qoe9/public/g2tfqi78/	Get hash	malicious	Browse	• 195.74.38.63
	http://https://handesign.vn/qcu/statement/	Get hash	malicious	Browse	• 195.74.38.63

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	64361
Entropy (8bit):	7.684495659223058
Encrypted:	false
SSDEEP:	1536:cn0WhVYfJctSVxFbp9OfifeAftApi2S2IP1YS:cn0WhqESVxFvOfiffFWplVIP1n
MD5:	0C9FEA6962FEF69F82CBF6D43D385D72
SHA1:	F5C8EB4A6428250723B78ABE0AD4E485D5CB9A3F
SHA-256:	F9517887432082174F7A7829347015A17D8BB71C7478DC1A582ABC6A41DE0B0A
SHA-512:	03DD6D5E1E99CA7D4C001626340E70BAB78DFC97ADF1BF15C40110775C635E161783FC72D490811F06CA2D770437B80C9B5FDCCB2CC394E9AD03781198B5DCD
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....C...l?&..an.0.....#z"..G.5.#D.....J..e....X.l8%.w.-.Zj.4.....[...S...+..... "... .Zt/g...lz...:e.....x0.....:V]..R-.6..u~...n.!B0Z.D...S{j.Zi...Kf..... Y...c..... C3. .D...B.c..._.7...^..p.i..VP..~.Km..O>....\$.5!\$..o....8.4@kB.g.G...y..x....n.\$x.G.=...3.63...r.!...../..o..L..5.gN#.R.E.u..xvg7.{...}[...>.M.Ja.uO'.....iV.F...x...<.....AL... wh...4.N.../_...m^g.....PK.....!..%b.....[Content_Types].xml ...[.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Mon Feb 22 16:08:42 2021, atime=Mon Feb 22 16:08:42 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.488795912986052
Encrypted:	false
SSDEEP:	12:85QXXEcLgXg/XAICPChaX2B8GB/wUoXx+Wnicvb0nbDIz3YilMMEpxRljKRlCTdK:858XV/XtM6GGJYelbDv3qsArNru/
MD5:	B416ED716D7E12B6B0552A760914215B
SHA1:	A18D44980D4B643E9C63A9DAB00ECC701AC67DA3
SHA-256:	7C66EE00CC6C3D064644589E387F927968475FF2C65AA842B53F085BF52AAB50
SHA-512:	37115F9FA4D98642419E87B31051894E2337439735B13208F5189A525EDAEOC478A99B32C6FE085097C56623C13F790539784A6E5B1342275A2E59365B6398DF
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..vxE_=...vxE_=.....i....P.O. :i.....+00.../C:\.....t1....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....VR....Desktop.d.....QK.XVR.*_...=.....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\.#.....\841675\Users.user\Desktop.....\.....\.....\D.e.s.k.t.o.p.....(,LB.)...Ag.....1SPS.XF.L 8C....&m.m.....-S.-1.-5.-2.1.-9.6.6.7.7.1.3.1.5.-3.0.1.9.4.0.5.6.3.7.-3.6.7.3.3.6.4.7.7.-1.0.0.6.....`.....X.....841675.....D_....3N...W...9r.[*.....}EkD_....3N.. .W...9r.[*.....}Ek...

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1019153116.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCELE.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:17 2020, mtime=Mon Feb 22 16:08:42 2021, atime=Mon Feb 22 16:08:42 2021, length=91136, window=hide
Category:	dropped
Size (bytes):	2118
Entropy (8bit):	4.503765643439255
Encrypted:	false
SSDEEP:	48:8zr/XTFGq3Bh5BEsAQh2zr/XTFGq3Bh5BEsAQ/:8zr/XJGqxNEvQh2zr/XJGqxNEvQ/
MD5:	E0AA4165386E623CEB069A0D7BA6499C
SHA1:	0C3B1760457822F8276FFE703E03AD0A8B0F7815
SHA-256:	39E0BC22279877DF21EDCC70BC5B676510717D5BE71D8A55290465892DE331BD
SHA-512:	53643399F3E62D44AB2B1E3359C9C68253BE87CB7EF7F5BE518206B4325963A846A91C7A6CDE219E9C442219F3DAB732B47BC15D92BD7C2C725CE3AF65C5AB13
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1019153116.LNK	
Preview:	L.....F.....g+..{..vxE_=_X_Q_=_...d.....P.O..i.....+00.../C\.....t1.....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.....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.....x.2..d.VR..._DOCUME~1.XLS..\.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.-1.0.1.9.1.5.3.1.1.6...x.l.s.....8..[.....?J.....C:\Users\.#.....\841675\Users.user\Desktop\document-1019153116.xls.....\.....\.....\.....\D.e.s.k.t.o.p\l.d.o.c.u.m.e.n.t.-1.0.1.9.1.5.3.1.1.6...x.l.s.....(.....LB.)...A.g.....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.....841675.....D_...3N.

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):	110
Entropy (8bit):	4.657921932424814
Encrypted:	false
SSDEEP:	3:oyBVomMY9LRqpFoZELRqpFomMY9LRqpFov:dj6Y9LQpFSELQpF6Y9LQpFy
MD5:	AD54D28BC72BB3AE0B8D6F3A02779930
SHA1:	1B7BCAA8E0AA9C6816C87632204CECDBD5606B6B
SHA-256:	FB0FF89328C6F3B88606C388F987C095307B800A0FF7B19ECDE6A4E315F5620B
SHA-512:	184158C298210DA588B8FAEF8ABB3BAB6937A7AB48902453373A2A02990B0F02E1BB1B556253151042ACB7D8A58E96813441BE65BF38D96664A69892F626D9A7
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-1019153116.LNK=0..document-1019153116.LNK=0..[xls]..document-1019153116.LNK=0..

C:\Users\user\Desktop\50EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	124228
Entropy (8bit):	4.293071155115131
Encrypted:	false
SSDEEP:	3072:uKcKoSsxzNDZLDZjlbR868O8KL5L+FxEtjPOtioVjDGUU1qfDlaGGx+cL2QnAFVO:pcKoSsxzNDZLDZjlbR868O8KL5L+FxEx
MD5:	AB6EE87A875CC6F92D281823CD4DFB93
SHA1:	563F9324E226B66488AFEA36343037C0E2C8041B
SHA-256:	191D1662946EA2EBE54A2BAEB8570C010419278BEBE617C4F13E6146A269C094
SHA-512:	61A4AD6D235E1BC933D1528B52DEA9913B2E7F72623FB4ABE443ECAD5E5618DCCBA1655BA08DF8EF99BD8BFE30DD0259AEF0CB7C68258C96D388E5C48955EE24
Malicious:	false
Reputation:	low
Preview:	g2.....\p....B....a.....=.....i.9J.8.....X.@....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r. i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C.a l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

Static File Info

General	
File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Fri Feb 19 09:21:15 2021, Security: 0
Entropy (8bit):	3.440161290247343
TrID:	- Microsoft Excel sheet (30009/1) 78.94% - Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1019153116.xls
File size:	91136
MD5:	948a7b1bc28afb293af7f3fe933e11b83
SHA1:	8f858737a636e731b1b1220fd80d3234052fdf98
SHA256:	4e657cfccfd1d18b8166a8adb446bf8cf82e4ad20c178689c3cb872ca1b059092
SHA512:	cee16e7286ac47086a5432b7866d6295e2baa7f081784cb8149379d327d884eaf7b434bc8d2dd6c4d0eaaaf4178eb7fcb88ed9f5a49300f00fedc8989898df622

General	
SSDEEP:	1536:fEcKoSsxz1PDZLDZjlbR868O8KIVH347uDphYHc eXVhca+fMHLtyeGxcl8O9pTIQ:fEcKoSsxzNDZLDZjlbR 868O8KIVH347d
File Content Preview:	>.....

File Icon

	
Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1019153116.xls"

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

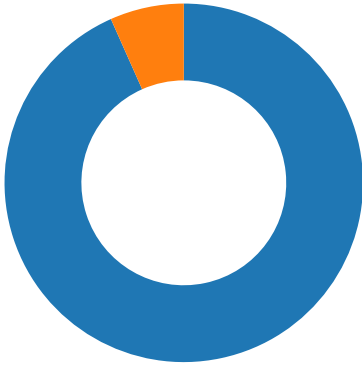
Summary	
Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-02-19 09:21:15
Creating Application:	Microsoft Excel
Security:	0

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

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.318330155209
Base64 Encoded:	False
Data ASCII:	+,...0.....H.....P..... ..X.....\.....h.....p.....x.....DocuSign.....Doc2.....Doc1.....Exc



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 09:08:42.939394951 CET	49167	443	192.168.2.22	195.74.38.127
Feb 22, 2021 09:08:43.007725954 CET	443	49167	195.74.38.127	192.168.2.22
Feb 22, 2021 09:08:43.007853031 CET	49167	443	192.168.2.22	195.74.38.127
Feb 22, 2021 09:08:43.025496960 CET	49167	443	192.168.2.22	195.74.38.127
Feb 22, 2021 09:08:43.092170954 CET	443	49167	195.74.38.127	192.168.2.22
Feb 22, 2021 09:08:43.092192888 CET	443	49167	195.74.38.127	192.168.2.22
Feb 22, 2021 09:08:43.092308998 CET	49167	443	192.168.2.22	195.74.38.127
Feb 22, 2021 09:08:43.093262911 CET	49167	443	192.168.2.22	195.74.38.127
Feb 22, 2021 09:08:43.094603062 CET	49168	443	192.168.2.22	195.74.38.127
Feb 22, 2021 09:08:43.159329891 CET	443	49167	195.74.38.127	192.168.2.22
Feb 22, 2021 09:08:43.160475969 CET	443	49168	195.74.38.127	192.168.2.22
Feb 22, 2021 09:08:43.160562038 CET	49168	443	192.168.2.22	195.74.38.127
Feb 22, 2021 09:08:43.165435076 CET	49168	443	192.168.2.22	195.74.38.127
Feb 22, 2021 09:08:43.229302883 CET	443	49168	195.74.38.127	192.168.2.22
Feb 22, 2021 09:08:43.229334116 CET	443	49168	195.74.38.127	192.168.2.22
Feb 22, 2021 09:08:43.229525089 CET	49168	443	192.168.2.22	195.74.38.127
Feb 22, 2021 09:08:43.230047941 CET	49168	443	192.168.2.22	195.74.38.127
Feb 22, 2021 09:08:43.231520891 CET	49169	443	192.168.2.22	195.74.38.127
Feb 22, 2021 09:08:43.298122883 CET	443	49168	195.74.38.127	192.168.2.22
Feb 22, 2021 09:08:43.299741030 CET	443	49169	195.74.38.127	192.168.2.22
Feb 22, 2021 09:08:43.299828053 CET	49169	443	192.168.2.22	195.74.38.127
Feb 22, 2021 09:08:43.300626993 CET	49169	443	192.168.2.22	195.74.38.127
Feb 22, 2021 09:08:43.368030071 CET	443	49169	195.74.38.127	192.168.2.22
Feb 22, 2021 09:08:43.368251085 CET	49169	443	192.168.2.22	195.74.38.127

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 09:08:42.839735985 CET	52197	53	192.168.2.22	8.8.8.8
Feb 22, 2021 09:08:42.927159071 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 09:08:42.839735985 CET	192.168.2.22	8.8.8.8	0xbf29	Standard query (0)	marknadsun dersokning.nu	A (IP address)	IN (0x0001)

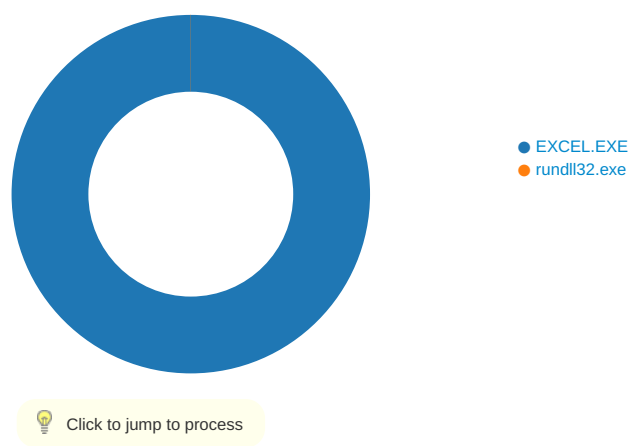
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 09:08:42.927159071 CET	8.8.8.8	192.168.2.22	0xbf29	No error (0)	marknadsun dersokning.nu		195.74.38.127	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2268 Parent PID: 584

General

Start time:	09:08:40
Start date:	22/02/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f0a0000
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\DE9C.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	13F3EEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\7FDE0000	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	7FEEAA29AC0	unknown

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	13FDC828C	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	13FDC828C	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	13FDC828C	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	13FDC828C	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	13FDC828C	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	13FDC828C	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	13FDC828C	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	13FDC828C	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	13FDC828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\621E.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	13F3EEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DE9C.tmp	success or wait	1	13F65B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image007.pn~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\621E.tmp	success or wait	1	13F65B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7FDE0000	C:\Users\user\AppData\Local\Temp\ism.sheet.csv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\50EE0000	C:\Users\user\Desktop\document-1019153116.xls.	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\mgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\mgs_files\stylesheet.cs~.	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\mgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\mgs_files\tabstrip.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\mgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\mgs_files\sheet001.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\mgs_files\image002.png	C:\Users\user\AppData\Local\Temp\mgs_files\image002.pn~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\mgs_files\image007.png	C:\Users\user\AppData\Local\Temp\mgs_files\image007.pn~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\mgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\mgs_files\sheet002.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\mgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\mgs_files\filelist.xm~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\mgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\mgs_files\stylesheet.css..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\mgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\mgs_files\tabstrip.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\mgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\mgs_files\sheet001.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\mgs_files\image008.pn_	C:\Users\user\AppData\Local\Temp\mgs_files\image008.pngss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\mgs_files\image009.pn_	C:\Users\user\AppData\Local\Temp\mgs_files\image009.pngss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\mgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Temp\mgs_files\sheet002.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\mgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\mgs_files\filelist.xmlss	success or wait	1	7FEEAA29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7FDE0000	569	454	c4 55 c9 6e db 30 10 bd 17 e8 3f 08 bc 16 12 9d 1c 8a a2 b0 9c 43 9a 1e db 00 49 3f 80 26 c7 12 61 6e e0 30 89 fd f7 1d d2 8a 9a 18 8e 15 23 06 7a f1 22 ea ad 14 47 f3 ab 8d 35 d5 23 44 d4 de b5 ec a2 99 b1 0a 9c f4 4a bb ae 65 7f ee 7f d6 d7 58 85 49 38 25 8c 77 d0 b2 2d 20 bb 5a 7c fe 34 bf df 06 c0 8a d0 0e 5b d6 a7 14 be 73 8e b2 07 2b b0 f1 01 1c ad ac 7c b4 22 d1 df d8 f1 20 e4 5a 74 c0 2f 67 b3 af 5c 7a 97 c0 a5 3a 65 0e b6 98 ff 80 95 78 30 a9 ba d9 d0 e5 9d 93 e0 3a 56 5d ef ee cb 52 2d d3 36 e3 f3 75 7e 10 b1 d4 6e 0f 21 42 30 5a 8a 44 d1 f8 a3 53 7b b6 6a bf 5a 69 09 ca cb 07 4b 66 1a 0c 11 84 c2 1e 20 59 d3 84 a8 c9 63 bc 83 94 a8 0a 7c 43 33 82 c1 d3 44 87 1e 1a 42 16 63 d8 eb 80 5f a8 ac 37 14 f2 ca eb 1e 5e a6 1a 70 bf 69 03 a3 56 50 dd 8a	.U.n.0....?.....C....!?.& ..an.0.....#z"...G...5. #D.....J..e.....X.l8%.w...- .Z .4.....[...s...+.....]."... .Zt./g..lz...e.....x 0.....:Vj...R-6..u~...n.lB 0Z.D...S{j.Zi....Kf..... Y.. ..c..... C3...D...B.c..._7.. ...^..p.i..VP..	success or wait	31	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\7FDE0000	1023	2	03 00	..	success or wait	20	7FEEAA29AC0	unknown

[illegible]

[illegible]

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\50EE0000	unknown	276	fe ff 00 00 06 01 02		success or wait	1	7FEEAA29AC0	unknown
			00 00 00 00 00 00 00	+...0.....				
			00 00 00 00 00 00 00	H.....P.....X.....`.....				
			00 00 00 01 00 00 00	.h.....p.....x.....				
			02 d5 cd d5 9c 2e 1b					
			10 93 97 08 00 2b 2c					
			f9 ae 30 00 00 00 e4	DocuSign.....Doc2.....Doc1				
			00 00 00 08 00 00 00	Worksheets.....				
			01 00 00 00 48 00 00	Excel				
			00 17 00 00 00 50 00					
			00 00 0b 00 00 00 58					
			00 00 00 10 00 00 00					
			60 00 00 00 13 00 00					
			00 68 00 00 00 16 00					
			00 00 70 00 00 00 0d					
			00 00 00 78 00 00 00					
			0c 00 00 00 9f 00 00					
			00 02 00 00 00 e4 04					
			00 00 03 00 00 00 00					
			00 0e 00 0b 00 00 00					
			00 00 00 00 0b 00 00					
			00 00 00 00 00 0b 00					
			00 00 00 00 00 00 0b					
			00 00 00 00 00 00 00					
			1e 10 00 00 03 00 00					
			00 09 00 00 00 44 6f					
			63 75 53 69 67 6e 00					
			05 00 00 00 44 6f 63					
			32 00 05 00 00 00 44					
			6f 63 31 00 0c 10 00					
			00 04 00 00 00 1e 00					
			00 00 0b 00 00 00 57					
			6f 72 6b 73 68 65 65					
			74 73 00 03 00 00 00					
			02 00 00 00 1e 00 00					
			00 11 00 00 00 45 78					
			63 65 6c					
C:\Users\user\Desktop\50EE0000	unknown	1536	01 00 00 00 02 00 00		success or wait	1	7FEEAA29AC0	unknown
			00 03 00 00 00 04 00					
			00 00 05 00 00 00 06					
			00 00 00 07 00 00 00					
			08 00 00 00 09 00 00	..!..."...#...\$...%...&...'...				
			00 0a 00 00 00 0b 00	(...)*...+...-...				
			00 00 0c 00 00 00 0d	.../...0...1...2...3...4...5.				
			00 00 00 0e 00 00 00	..6...7...8...9...:;...<...				
			0f 00 00 00 10 00 00	=...>...?...@...				
			00 11 00 00 00 12 00					
			00 00 13 00 00 00 14					
			00 00 00 15 00 00 00					
			16 00 00 00 17 00 00					
			00 18 00 00 00 19 00					
			00 00 1a 00 00 00 1b					
			00 00 00 1c 00 00 00					
			1d 00 00 00 1e 00 00					
			00 1f 00 00 00 20 00					
			00 00 21 00 00 00 22					
			00 00 00 23 00 00 00					
			24 00 00 00 25 00 00					
			00 26 00 00 00 27 00					
			00 00 28 00 00 00 29					
			00 00 00 2a 00 00 00					
			2b 00 00 00 2c 00 00					
			00 2d 00 00 00 2e 00					
			00 00 2f 00 00 00 30					
			00 00 00 31 00 00 00					
			32 00 00 00 33 00 00					
			00 34 00 00 00 35 00					
			00 00 36 00 00 00 37					
			00 00 00 38 00 00 00					
			39 00 00 00 3a 00 00					
			00 3b 00 00 00 3c 00					
			00 00 3d 00 00 00 3e					
			00 00 00 3f 00 00 00					
			40 00 00					

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAA29AC0	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\5367203117.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAA29AC0	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\5367203117.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	1	7FEEAA29AC0	unknown

[illegible]

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

Analysis Process: rundll32.exe PID: 2028 Parent PID: 2268

General

Start time:	09:08:43
Start date:	22/02/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..iopjvdf.vock,DllRegisterServer
Imagebase:	0xff4b0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

Disassembly

Code Analysis