ID: 686026
Sample Name: C1ZGt61uGv
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 04:22:09
Date: 18/08/2022
Version: 35.0.0 Citrine

Table of Contents

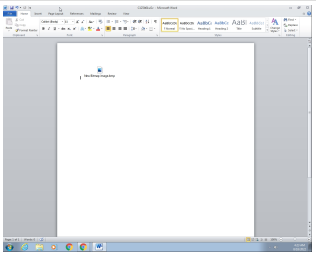
Windows Analysis Report

C1ZGt61uGv

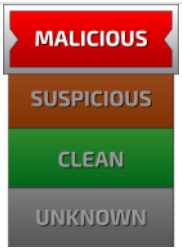
Overview

General Information

Sample Name:	C1ZGt61uGv (renamed file extension from none to docx)
Analysis ID:	686026
MD5:	98998af843c2c9…
SHA1:	b1a1dda90b3df0..
SHA256:	b0cfd511498cba…
Infos:	



Detection



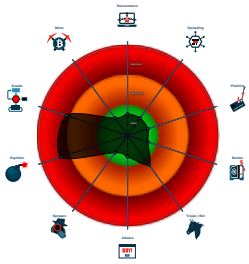
Follina CVE-2022-30190

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Microsoft Office Expl…
- Malicious sample detected (through…
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Contains an external reference to an…
- Detected suspicious Microsoft Offic…
- Yara signature match
- Potential document exploit detected…
- Uses a known web browser user age…
- JA3 SSL client fingerprint seen in co…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2960 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:$a1: <Relationships • 0x3d2:$a2: TargetMode="External" • 0x3ca:$x1: .html!
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x375:$olerel: relationships/oleObject • 0x38e:$target1: Target="http • 0x3d2:$mode: TargetMode="External

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
sslproxydump.pcap	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x2d0d:$a: PCWDiagnostic • 0x6177:$a: PCWDiagnostic • 0x2d01:$sa3: ms-msdt • 0x616b:$sa3: ms-msdt • 0x2d61:$sb3: IT_BrowseForFile= • 0x61cb:$sb3: IT_BrowseForFile=
sslproxydump.pcap	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\index[1].htm	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x1444:$a: PCWDiagnostic • 0x1438:$sa3: ms-msdt • 0x1498:$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\index[1].htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1427:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\index[1].htm	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x1444:$a: PCWDiagnostic • 0x1438:$sa3: ms-msdt • 0x1498:$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\index[1].htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1427:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\index[1].htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Click to see the 7 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Powershell commands sent B64 1 - Source IP: 35.186.245.55 - Destination IP: 192.168.2.22

Timestamp:	35.186.245.55192.168.2.22443491762025010 08/18/22-04:23:24.931708
SID:	2025010
Source Port:	443
Destination Port:	49176
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Powershell commands sent B64 1 - Source IP: 35.186.245.55 - Destination IP: 192.168.2.22

Timestamp:	35.186.245.55192.168.2.22443491812025010 08/18/22-04:23:28.806682
SID:	2025010
Source Port:	443
Destination Port:	49181
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Antivirus detection for dropped file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected suspicious Microsoft Office reference URL

Networking

Snort IDS alert for network traffic

System Summary

Malicious sample detected (through community Yara rule)

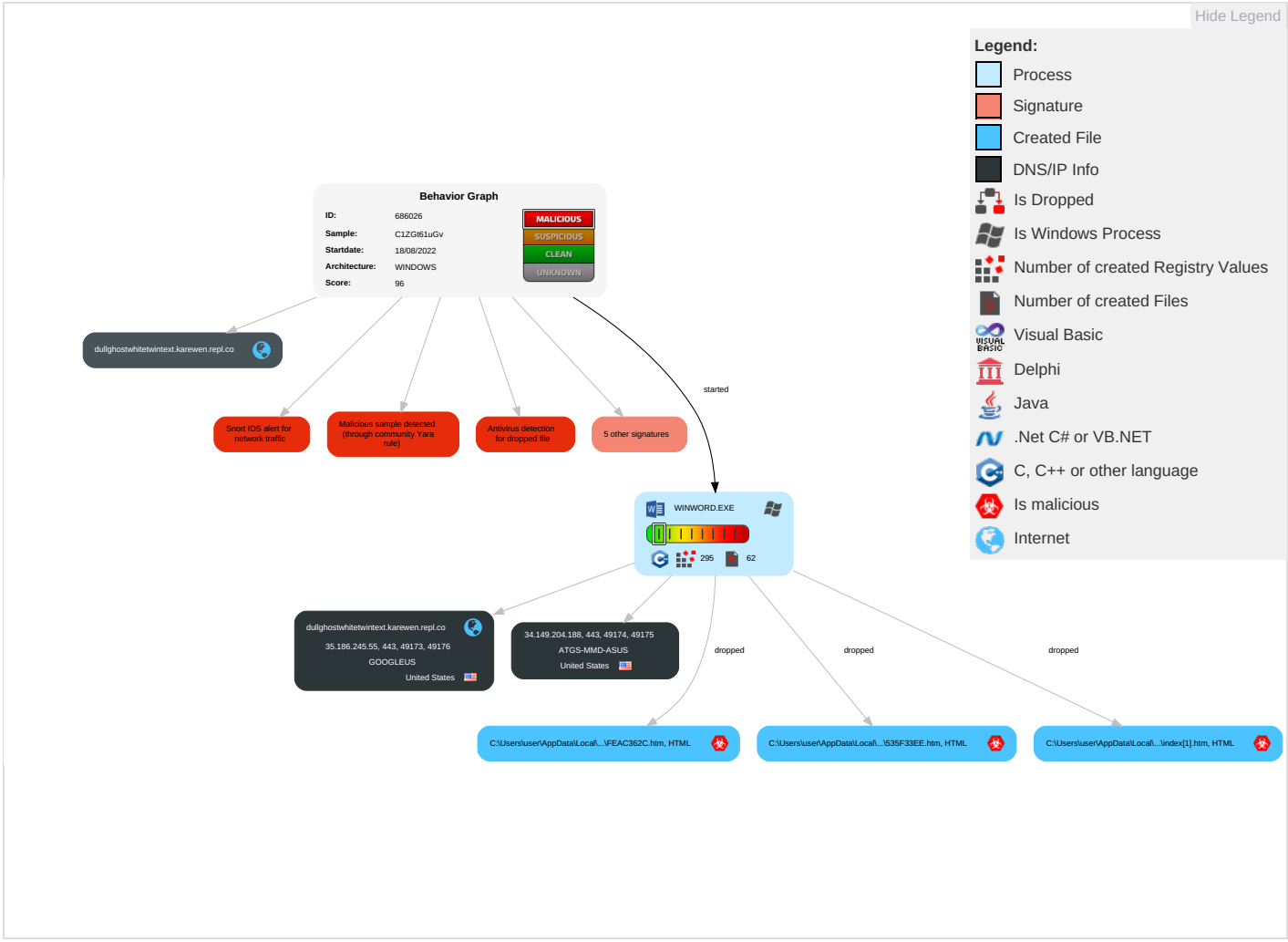
Persistence and Installation Behavior

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 3 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	1 Encrypted Channel	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	2 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-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	1 4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	4 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

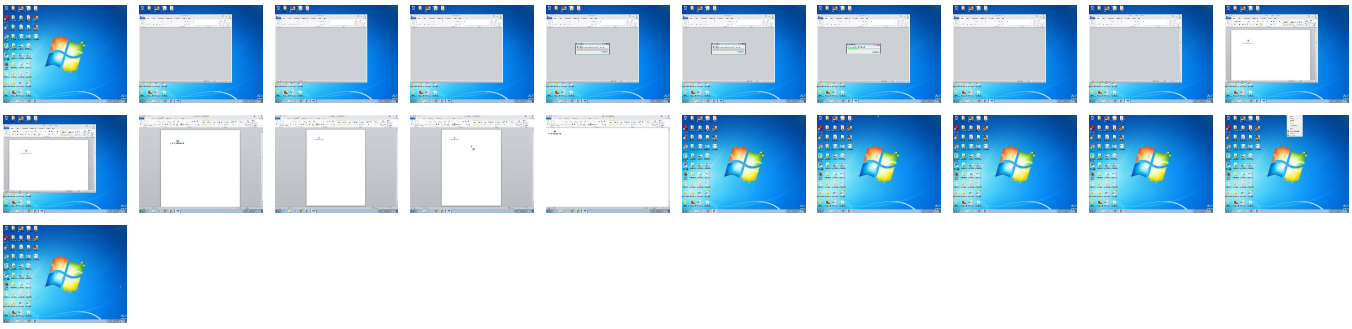
Behavior Graph

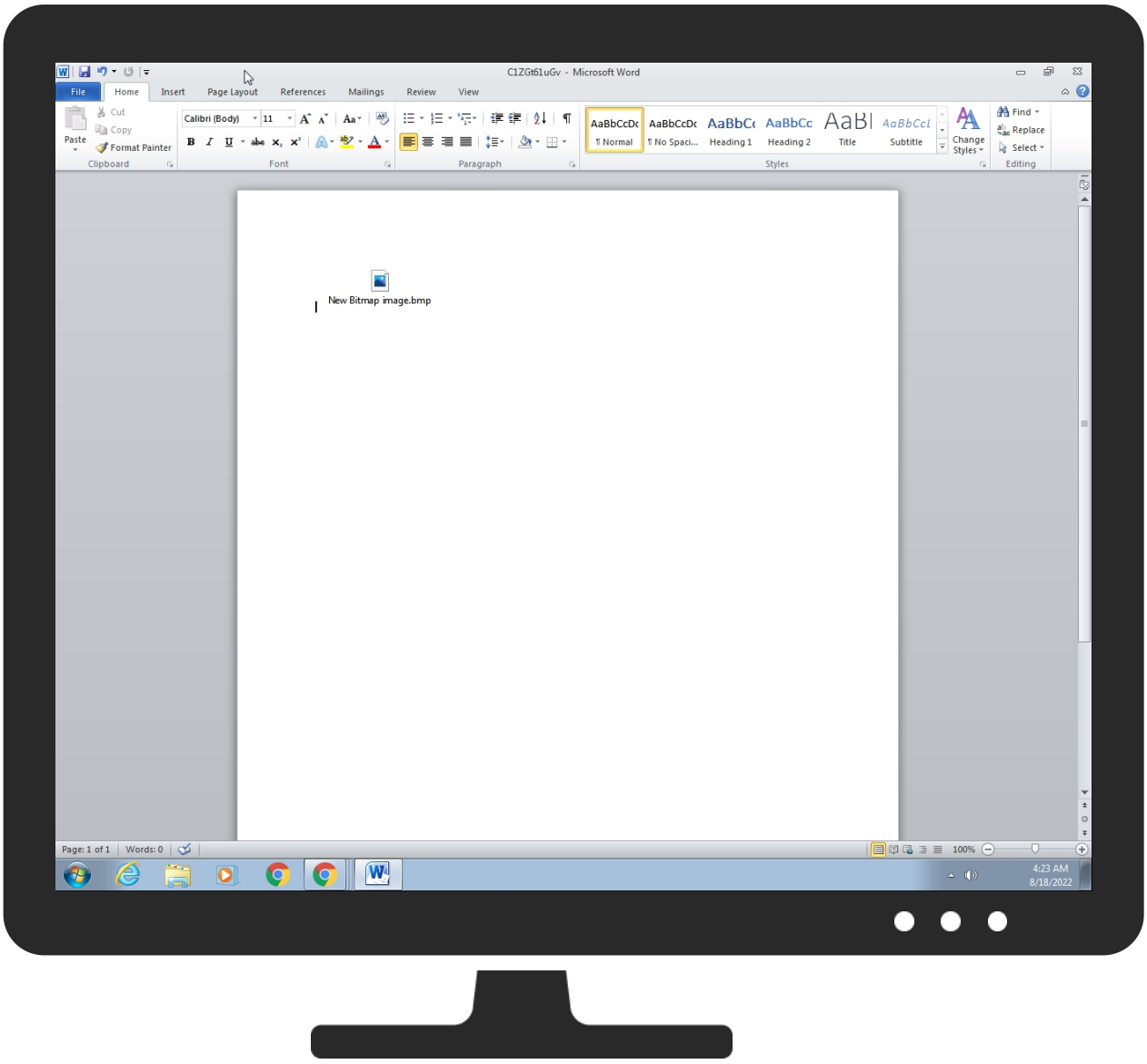


Screenshots

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
C1ZGt61uGv.docx	46%	Virustotal		Browse
C1ZGt61uGv.docx	26%	Metadefender		Browse
C1ZGt61uGv.docx	35%	ReversingLabs	Document-Word.Trojan.Minerva	
C1ZGt61uGv.docx	100%	Avira	W97M/Dldr.Agent.G1	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\535F33EE.htm	100%	Avira	JS/CVE-2022-30190.G	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\index[1].htm	100%	Avira	JS/CVE-2022-30190.G	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\index[1].htm	100%	Avira	JS/CVE-2022-30190.G	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FEAC362C.htm	100%	Avira	JS/CVE-2022-30190.G	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dullghostwhitetwintext.karewen.repl.co	35.186.245.55	true	false		high

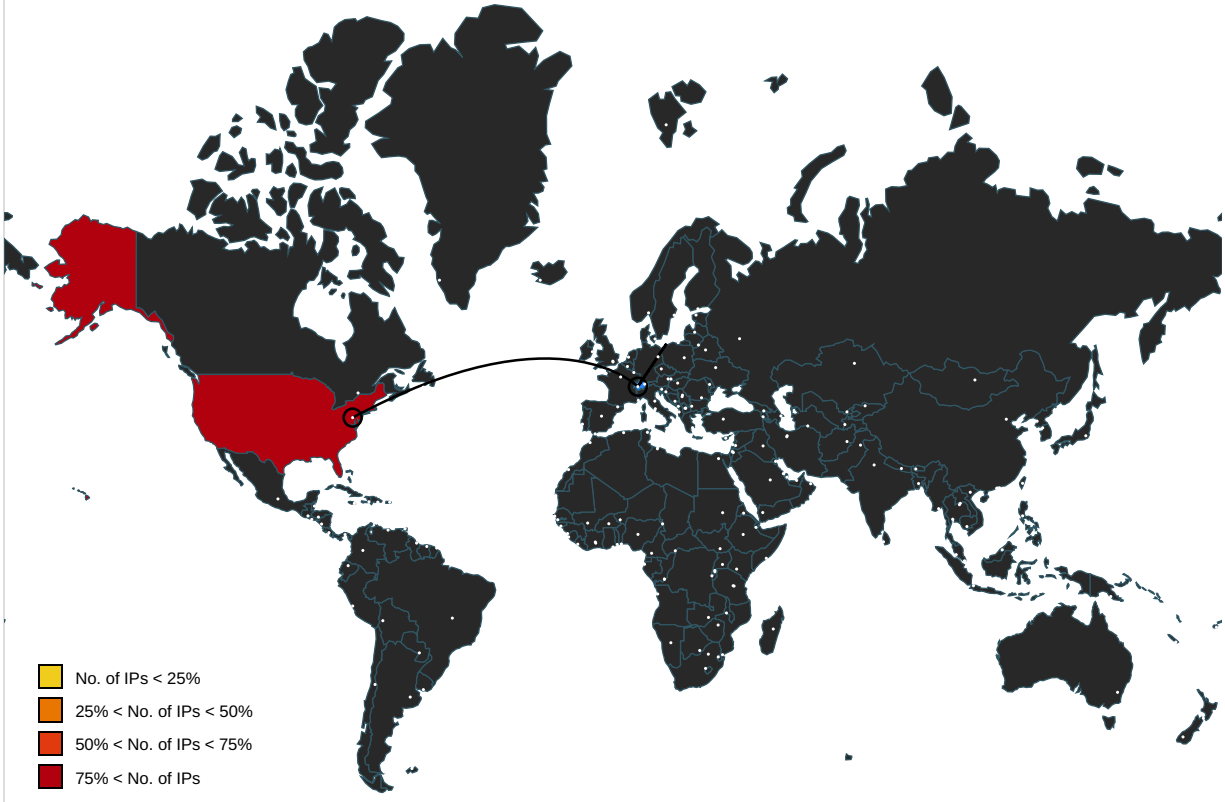
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://dullghostwhitetwintext.karewen.repl.co/index.html	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dullghostwhitetwintext.karewen.repl.co/index.htmlyX	~WRF{4AF4D387-AD82-4BF6-994E-7F9F57B3DDFD}.tmp.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
35.186.245.55	dullghostwhitetwintext.karewen.repl.co	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.149.204.188	unknown	United States		2686	ATGS-MMD-ASUS	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	686026
Start date and time:	2022-08-18 04:22:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	C1ZGt61uGv (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:	6
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:	mal96.expl.evad.winDOCX@1/20@7/2
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
- TCP Packets have been reduced to 100
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too 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):	0.28773612475316834
Encrypted:	false
SSDEEP:	24:I3yC/9LC4tB37+KqorUSjnClWnyc8v5TbT/tAZvzKxFcNTRxlQvnS8S9XqJNQSEQ:I35RBzAccmKyTjlJQaxwOr0JZH
MD5:	FF3458BF59CAB2B33042A43FE7571C5E
SHA1:	B8B002E94BF658303BE1DA5E7D5FA7670EA882B7
SHA-256:	E151CF032E1294178D66CF5D065FD8F0C26D27945195FD34738910D25B6A567D
SHA-512:	256C055110B1AA138F19FC4519D05FE158FBCEF88C8E604DECE24FF2AAB6808208E9DED419613436E08DB2429124F131F2E5F81FCDFC3C9C0E1CE1240F0EC22
Malicious:	false
Reputation:	low
Preview:	......M.eFy...zk9ln...H...J../.S,...X.F...Fa.q.....!.);.N...?...L.....+9....D..r..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\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.6745976468464878
Encrypted:	false
SSDEEP:	768:T5K146vqOVHUvJBmtlK2DrxtlK2DrwZPJl/XDr/klmDr/4xtD+DrbtDlDr:Lhw
MD5:	9F01FC48E22641773BC5DB74B89EB0E1
SHA1:	B4985AF395531C350958A267B7D81F78AABA57A2
SHA-256:	0E19C09DC2C68235B7C39C13A81A3125C376D9135267CB003B1057285581374B
SHA-512:	BCA4CA34F6F4DCF49EF55B53FF8C9F1452BCE4A6426B083FC7AFA578CD88C07635E12844AA63319E5CC21128EB2F7FCD1066FD7DAE453A1720333FA41445A9E2
Malicious:	false
Reputation:	low
Preview:	......M.eFy...zM..7..+M....L..NS,...X.F...Fa.q.....J....@.B.H.....).%5VJ... .....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):	3.936756154878342
Encrypted:	false
SSDEEP:	3:yVlgsRlzXh4NaPlDpKQclkrI8TcOhFYDZ276:yPblzXeWl0J+c8QGFYDZ22
MD5:	508E494841A8C3839E148679A4937283
SHA1:	668677B7DBA2DBD40A596A200D0176B965BD44AE
SHA-256:	AB0AE8DEF878D06C5F65D16C14B4ACBEE7EED1666584865D90C62E5704B5B48A
SHA-512:	DABFFDCCE773E059F52E137EAE54621AE36E33CB28A5A6A86CC5E323D23A8ACDB3B8B76CB74CC9BFDFC8586A0D2BF553FE63C40F5B1D3CCB197A6721E1ED644A
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.8.2.D.6.D.0.4.A.-.E.2.A.7.-.4.2.F.1.-.8.9.A.6.-.C.F.D.5.7.F.9.E.C.7.6.6.}...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):	0.28745721354451365
Encrypted:	false
SSDEEP:	48:I3sPRBffmW1AEr12ORQopWi3hI9ahlrq1/Tp9oipEGQO09oipEGQOyH:KoLXYErFHI9aXq1DmbBmbvH
MD5:	5F39A4DAC8039EB065DD8D063640BC4F
SHA1:	BBEA611DA4F133FB3F02C273B60D379060ECC49C
SHA-256:	FA8BE565755B84D32FF994D075AF5002629176DA9771B5CC9C78268C0021BACC
SHA-512:	5B983F376F0146604DA61EBED288E016E4DD43EA1A8971D3953DBC8D1B52B5BD22D88B32628A61EC06C784B14AC2B0A5F65AC8B128F3D84422861B0BE9BFBC2D
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z....H*.O...L..S,...X.F...Fa.q.....&.....F.~.c.....7..B.Z.../^T.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-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.22075992709284928
Encrypted:	false
SSDEEP:	48:I3oyQUrB/2aWIeFRmHaaGEW1+7DYd7z1IZuxTV/ZjA/iZjA/J:KoLCjuRQG7ZYuxT/AmAx
MD5:	B53D2E2D585B0857AAFF3A807DDDFE73
SHA1:	309EB90AD24B5FC926D00B6B16A2DE199522114E
SHA-256:	EE3835D8BE77FC46EB661A14ADCC3285582CC8774C8F2617922D99D5A13C29CE
SHA-512:	C8ACE3F93133C5F4C8E257D311DE4F182144F4871EDA19A18DD83BB0E05A433FA37F4440F8DA50C283FD720D6F4860B601B56F91D3C95BF56186674C8DBAE76
Malicious:	false
Reputation:	low
Preview:	......M.eFy...zI...ZSbO.*G..8.S,...X.F...Fa.q.....p..FG...+@.H.....d....$/H....N..-P>.....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):	3.92634307586349
Encrypted:	false
SSDEEP:	3:yVlgsRlz2rZjMWjjic+lIHdhHAWelOVG4R7276:yPblzwWDc19SWzk4t22
MD5:	63BA949A4695972C1A0E4D0BEC674841
SHA1:	6002A36601A9EEE1C8B4667761AF8815D4E6D8C9
SHA-256:	D5D97F1310E4BFA007D830CA4E1953DF22BE1B797B27692712F5C93E6DBC43DB
SHA-512:	2EE603F54070AA54538FCB3F8C541437E1BFA50E3F5638080135606935494 0FBFCCB116591D59B25D5F435255E0820DBFCB271EF975670FC91BD03D1D7D1A39D
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.E.C.A.F.6.F.F.3.-.F.9.C.F.-.4.9.5.B.-.8.0.D.B.-.8.0.3.5.D.E.A.3.0.9.E.7.}...F.S.D..

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	5901
Entropy (8bit):	4.701941274629396
Encrypted:	false
SSDEEP:	96:O/iGBF2nPW5mDwID8qImX1I8vHWYMLJJ2lpyffnbTc7Om/EAEwCgEAKKiSe+0glg:OZ5mDwIDukGTlKEHbTcKCZEwCgEzKiSs
MD5:	2C855A56E062B197D4CC9D021DF71219
SHA1:	C3161D4AF43AD3DA1B08FF367C06D12FA7D483D5
SHA-256:	A6F55957542982348EB412B9B49797E1931183A6BF395016885E1294C5A08DBD
SHA-512:	11B94B5B6E3F4AEC38B15BF73A3B6836955980F5A47293266BB1FAA88005C94EBBF57465D02D8D4CF164E3F28236A7190592CA6E8C3E82A98CBF7708CF1DCDC0
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\index[1].htm, Author: Nasreddine Bencherchali, Christian Burkard • 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\index[1].htm, Author: Tobias Michalski, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\index[1].htm, Author: Nasreddine Bencherchali, Christian Burkard • 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\index[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\index[1].htm, Author: Joe Security • 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\index[1].htm, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100%
Reputation:	low
IE Cache URL:	http://https://dullghostwhitetwintext.karewen.repl.co/index.html
Preview:	<!doctype html>.<html lang="en">.<head>.<title>.Good thing we disabled macros.</title>.</head>.<body>.<p>.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor...Curabitur rutrum leo tortor, venenatis fermentum ex portti tor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit...Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique ante, dignis

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	5901
Entropy (8bit):	4.701941274629396
Encrypted:	false
SSDEEP:	96:O/iGBF2nPW5mDwID8qImX1I8vHWYMLJJ2lpyffnbTc7Om/EAEwCgEAKKiSe+0glg:OZ5mDwIDukGTlKEHbTcKCZEwCgEzKiSs
MD5:	2C855A56E062B197D4CC9D021DF71219
SHA1:	C3161D4AF43AD3DA1B08FF367C06D12FA7D483D5
SHA-256:	A6F55957542982348EB412B9B49797E1931183A6BF395016885E1294C5A08DBD

SHA-512:	11B94B5B6E3F4AEC38B15BF73A3B6836955980F5A47293266BB1FAA88005C94EBBF57465D02D8D4CF164E3F28236A7190592CA6E8C3E82A98CBF7708CF1DCDC0
Malicious:	false
Reputation:	low
Preview:	<!doctype html>.<html lang="en">.<head>.<title>.Good thing we disabled macros.</title>.</head>.<body>.<p>.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor...Curabitur rutrum leo tortor, venenatis fermentum ex portti tor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit...Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique ante, dignis

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\535F33EE.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	5901
Entropy (8bit):	4.701941274629396
Encrypted:	false
SSDEEP:	96:O/iGBF2nPW5mDwID8qImX1I8vHWYMLJJ2lpyffnbTc7Om/EAEwCgEAKKiSe+0glg:OZ5mDwIDukGTlKEHbTcKCZEwCgEzKiSs
MD5:	2C855A56E062B197D4CC9D021DF71219
SHA1:	C3161D4AF43AD3DA1B08FF367C06D12FA7D483D5
SHA-256:	A6F55957542982348EB412B9B49797E1931183A6BF395016885E1294C5A08DBD
SHA-512:	11B94B5B6E3F4AEC38B15BF73A3B6836955980F5A47293266BB1FAA88005C94EBBF57465D02D8D4CF164E3F28236A7190592CA6E8C3E82A98CBF7708CF1DCDC0
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\535F33EE.htm, Author: Nasreddine Bencherchali, Christian Burkard • 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\535F33EE.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\535F33EE.htm, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	<!doctype html>.<html lang="en">.<head>.<title>.Good thing we disabled macros.</title>.</head>.<body>.<p>.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor...Curabitur rutrum leo tortor, venenatis fermentum ex portti tor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit...Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique ante, dignis

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AC592AE0.emf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	10172
Entropy (8bit):	3.928478624213631
Encrypted:	false
SSDEEP:	48:q373cifeyUaIWmBJOhTDOj1WN7M60iIiB7rSwVauLM/Myof9NLRgMy7k3e2kW86J:873xeXaIBckry+Ks8D+plS
MD5:	C349F98D0BBE0D72F9A6E34335918207
SHA1:	B2184C336F95E1ED5F338D1B27D06A4F8E1C535F
SHA-256:	8ACC7CBE7BEB283D3908F418FB5390623F1EB46018F426D4911F5515E786CAA5
SHA-512:	A6DE09C1E4B3947EF4B8BF46B14A3E77AFFB6004EDED3560814720B8304542F1722EFEF83502E0532C76B438015B84200302BE5CE5F8C1228A881F050BE8AE5B
Malicious:	false
Reputation:	low
Preview:	....l.....l.....'...9... EMF.....'.....8...5.....R...R...p.....S.e.g.o.e. .U.l.....dv.....%.....r....$..`...../...`.....0...0.....?.....?.....l...4.....$..0...0...(...0...0..... .....$.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FEAC362C.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	5901

Entropy (8bit):	4.701941274629396
Encrypted:	false
SSDEEP:	96:O/iGBF2nPW5mDwID8qImX1I8vHWYMLJJ2lpyffnbTc7Om/EAEwCgEAKKiSe+0glg:OZ5mDwIDukGTlKEHbTcKCZEwCgEzKiSs
MD5:	2C855A56E062B197D4CC9D021DF71219
SHA1:	C3161D4AF43AD3DA1B08FF367C06D12FA7D483D5
SHA-256:	A6F55957542982348EB412B9B49797E1931183A6BF395016885E1294C5A08DBD
SHA-512:	11B94B5B6E3F4AEC38B15BF73A3B6836955980F5A47293266BB1FAA88005C94EBBF57465D02D8D4CF164E3F28236A7190592CA6E8C3E82A98CBF7708CF1DCDC0
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FEAC362C.htm, Author: Nasreddine Bencherchali, Christian Burkard • 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\FEAC362C.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\FEAC362C.htm, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	<!doctype html>.<html lang="en">.<head>.<title>.Good thing we disabled macros.</title>.</head>.<body>.<p>.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor...Curabitur rutrum leo tortor, venenatis fermentum ex portti tor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit...Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique ante, dignis

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4AF4D387-AD82-4BF6-994E-7F9F57B3DDFD}.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):	5632
Entropy (8bit):	2.181448160411441
Encrypted:	false
SSDEEP:	48:rMTLxD3U2557fpQ0fpQRiVDaU2557fpQAfpQFi:QTLxD3U2TenAVDaU2Ter0
MD5:	4B4FEA476768A33C0BCF51BCDDB2CCD4
SHA1:	80D924A68CBE3D1CAA003D7180A3FB3713A15F30
SHA-256:	675CDC18EB9F7FA3C1C4287FF4C1CFADFB81B54073AF377D5082BD23B0D472CD
SHA-512:	20B06E268A0343D559C140BF525E4C0915EB9B5BDA33D94BC51E5B19EBEE3C725CD2E0D1BF75D34E9E4C984F32E0CA0356D85378CECD8DE1EA44ED38EEB68A24
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{92861601-980D-49B7-B60E-86BDABC4A51A}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D894BCB6-25AA-45DC-81E3-B0273BF56D57}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	0.9434685449697431
Encrypted:	false
SSDEEP:	6:FlIcElClbY/z35lEHaAlPrP5llAabK/O3iuzxyn4PxZUtg:Fl7MClcFlEHaAPrzXKzut8GZz
MD5:	4D066506FC8303FE21BD33D70AD15382
SHA1:	FBEB98890B56989FBDD274982690F11DA6EF3B8E
SHA-256:	D210EDD7CC5EEC6A9C3AD9C09B2755B8144C3A5ED44B178FE1EE3A50852E7B38
SHA-512:	05B05479DE9EE50CA74A890D27634A065995D34601343F059B8B66516FAAC79098CB4F9ADABFB3ED5CA763BF67A953260FFAA36D24A3BABC04FBA22BC9541FC5
Malicious:	false
Preview:	....L.I.N.K. .P.a.c.k.a.g.e. .".h.t.t.p.s.:././.d.u.l.l.g.h.o.s.t.w.h.i.t.e.t.w.i.n.t.e.x.t...k.a.r.e.w.e.n...r.e.p.l...c.o./.i.n.d.e.x...h.t.m.l.!.". ."."..\.b..... . ...

C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.02572382778486038
Encrypted:	false
SSDEEP:	6:I3DPcrHavxggLRxv26Lt3RXv//4tfnRujlw//+GtluJ/eRuj:I3DP2Hc/tRvYg3J/
MD5:	FAA9C11C3BF4749CF7FFF72F81103637
SHA1:	EA800893E160BDEC41C9E5A208ECDEFD93020DE4
SHA-256:	E4FE523DD900A6A9384D518919DC6F46F67E47BA19062D66BC33738FC9D63D7C
SHA-512:	89283E5CC4D45C886D88EDFF6DD6D81FFBD9DC643925411851E4EAE034BD56F8C9C60C932D6C8DE3A95DB20D06F0F0A4DBF4081CBFBAA03B174D061BA4A75A66
Malicious:	false
Preview:	......M.eFy...zk9ln...H...J./.S,...X.F...Fa.q.....fJ,....H.^...6.....+9....D..r..0.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025486724730822925
Encrypted:	false
SSDEEP:	6:I3DPc3vxggLReaZopSdh/RXv//4tfnRujlw//+GtluJ/eRuj:I3DPM6H2PvYg3J/
MD5:	DF1D9A5116232C0278742EE1F191FF0C
SHA1:	0BA0ABF8406B667D8C632F6B3ED6395430A0E8D1
SHA-256:	E4BC1D0AA363F21236E3EDF16C6863CB44D1A3E24B12EC190B33C8F19DF493A9
SHA-512:	35AE70F978C47590A32D185E04AA07C45647D8A9B42E0A1716E6AA1EE075A3F0CFF252FF1853A4C9E474C672F81DAB4022BA3AA37C5FDD1075413668015CB15B
Malicious:	false
Preview:	......M.eFy...z....H*.O...L..S,...X.F...Fa.q...../g.T.C.B.t.;.....7..B.Z.../^T.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\C1ZGt61uGv.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 Aug 18 10:22:03 2022, mtime=Thu Aug 18 10:22:03 2022, atime=Thu Aug 18 10:22:14 2022, length=26614, window=hide
Category:	dropped
Size (bytes):	1019
Entropy (8bit):	4.541555035737997

Encrypted:	false
SSDEEP:	12:8mbA80gXg/XAlCPCHaXNBQtB/XAJX+WuvWQK3juicvbTS3tb4GK/NDtZ3YilMMEh:8mb1k/XT9Sk+mNeHS3ADv3q+u7D
MD5:	16C92C158C9E519DF7E7171A87BA915B
SHA1:	5EA87A76FB2D1CB7776EE3E10902DB4D444EC686
SHA-256:	C3556B03AEDC5348C415F365D63B28E0DF81C86D721A2C8D1937AFDC46879F35
SHA-512:	BEFC41BCB397B893BFD14392992FC02FAD04AD946493E359E20DF11D3136DD145076148BA88B2BE3471D3709EA6EDC9B56EA90A02DC5F246BEE1E26F87CE18 3F
Malicious:	false
Preview:	L.....F.... ...^{(.....^{(.....g.....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.....U.Z..Desktop.d.....QK.X.U.Z*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-2. 1.7.6.9.....h.2..g...U.Z .C1ZGT6~1.DOC..L.....U.Z.U.Z*.....C.1.Z.G.t.6.1.u.G.v...d.o.c.x.....y.....-...8...[.....?J.....C:\Users\..#.....\\37714 2\Users.user\Desktop\C1ZGt61uGv.docx.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.1.Z.G.t.6.1.u.G.v...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.....377142.....D_....3N...W...9G..N..... .....[D_....3N...W...9G

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):	4.780851828270855
Encrypted:	false
SSDEEP:	3:bDuMJl+Uqe3TAlmxWtmx3TAlv:bCne3CE3W
MD5:	69F6516C10F77E405479AA56E74F44A0
SHA1:	36194337D22DE7E093B6659C3E3A1C98A2F243CE
SHA-256:	EFAE2CC5C7CBDFF13D4AC0A4FB3F0C0000C52A4E1C9AD499C834F0135A8ECCFB
SHA-512:	3443F8CF1E2804F86512DDDCEC8DF5F0F3683FA2D1E57FC4592E8A13FC7CCC9E402230D71F956DDB8D3873B6825979EB706599CB0F7B2FF32D1A993F31D945 B
Malicious:	false
Preview:	[folders]..Templates.LNK=0..C1ZGt61uGv.LNK=0..[misc]..C1ZGt61uGv.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):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265 5
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

C:\Users\user\Desktop\~$ZGt61uGv.docx

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265 5
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.316883678675453
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%
File name:	C1ZGt61uGv.docx
File size:	26614
MD5:	98998af843c2c938c079a102abe6c73d
SHA1:	b1a1dda90b3df0ba5f23430a6c55c48a9c3dbe9d
SHA256:	b0cfd511498cbaed084fa622cfeb1a07de7478205cbff58cb40cb89091813593
SHA512:	4b3fee7cddc41a3f742d2ca3bcc6db766e43d183b926153927ec5591d73cce2d0cf5b4ade9d0f010bf6b104f463d44e383e423984d0bf5684e58971dd0665ee7
SSDEEP:	384:aW5NndAzG46H8kwV1xEw2imBTQUhGnhHpAKIQqRrINxt/ZtNNiW2+30Ony/6MY:awlO1Ew2HGHiKpqRrSxlIN2+3By/e
TLSH:	DCC2C057D12B5C75CC6A4EBCD82C8ABCEA9430D0F9151187244DE6C9B24BD73133EA1A
File Content Preview:	PK.....!..l.$u.....[Content_Types].xml ... (.....

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/686026/sample/C1ZGt61uGv.docx"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	False

Summary

Title:	
Subject:	
Author:	Karewen .
Keywords:	
Template:	Normal.dotm
Last Saved By:	Karewen .
Revion Number:	2
Total Edit Time:	0
Create Time:	2022-06-03T10:03:00Z
Last Saved Time:	2022-06-03T10:03:00Z
Number of Pages:	1
Number of Words:	3
Number of Characters:	18

Creating Application:	Microsoft Office Word
Security:	0

Document Summary	
Number of Lines:	1
Number of Paragraphs:	1
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0000

Streams	
Stream Path: \x1CompObj, File Type: data, Stream Size: 76	
General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	76
Entropy:	3.093449526469053
Base64 Encoded:	False
Data ASCII:	. . . . . F . . . . O L E P a c k a g e . . . . . P a c k a g e . 9 q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 0c 00 03 00 00 00 00 00 c0 00 00 00 00 00 00 46 0c 00 00 00 4f 4c 45 20 50 61 63 6b 61 67 65 00 00 00 00 00 08 00 00 00 50 61 63 6b 61 67 65 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x10le10Native, File Type: data, Stream Size: 2240124	
General	
Stream Path:	\x1Ole10Native
File Type:	data
Stream Size:	2240124
Entropy:	0.005070123031127669
Base64 Encoded:	True
Data ASCII:	x . " . . . N e w B i t m a p i m a g e . b m p . D : \ \ S a y a a r \ \ P e r s o n a l \ \ C o d i n g \ \ M S D T Z e r o - D a y \ \ M S F o l l i n a \ \ N e w B i t m a p i m a g e . b m p . . . . . ^ . . . C : \ \ U s e r s \ \ k a r e w \ \ A p p D a t a \ \ L o c a l \ \ T e m p \ \ { 4 9 2 A 0 5 A 6 - 0 F C E - 4 3 E 2 - A F E 7 - D D 9 A E A 8 4 F C 1 B } \ \ N e w B i t m a p i m a g e . b m p . 6 , " . B M 6 , " . . . . . 6 . . . (. . . . . , " . . . . .
Data Raw:	78 2e 22 00 02 00 4e 65 77 20 42 69 74 6d 61 70 20 69 6d 61 67 65 2e 62 6d 70 00 44 3a 5c 53 61 79 61 61 72 5c 50 65 72 73 6f 6e 61 6c 5c 43 6f 64 69 6e 67 5c 4d 53 44 54 20 5a 65 72 6f 2d 44 61 79 5c 4d 53 46 6f 6c 6c 69 6e 61 5c 4e 65 77 20 42 69 74 6d 61 70 20 69 6d 61 67 65 2e 62 6d 70 00 00 00 03 00 5e 00 00 00 43 3a 5c 55 73 65 72 73 5c 6b 61 72 65 77 5c 41 70 70 44 61 74 61

Stream Path: \x3EPRINT, File Type: Windows Enhanced Metafile (EMF) image data version 0x10000, Stream Size: 10172	
General	
Stream Path:	\x3EPRINT
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Stream Size:	10172
Entropy:	3.928478624213631
Base64 Encoded:	False
Data ASCII:	. . . . l . . . . . l . . . . . ' . . . 9 . . . E M F . . . . ' . . . . . 8 . . . 5 . . . . . R . . . R . . . p . . . . . S . e . g . o . e . . U . l . . . . .
Data Raw:	01 00 00 00 6c 00 00 00 18 00 00 00 00 00 00 00 d7 00 00 00 49 00 00 00 00 00 00 00 00 00 00 00 27 0f 00 00 39 05 00 00 20 45 4d 46 00 00 01 00 bc 27 00 00 0d 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 07 00 00 38 04 00 00 35 01 00 00 ae 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 b7 04 00 b0 a7 02 00 0a 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 09 00 00 00

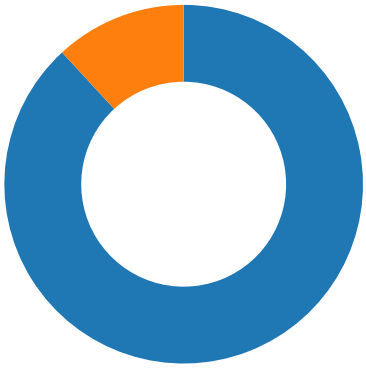
Stream Path: \x3ObjInfo, File Type: data, Stream Size: 6	
General	
Stream Path:	\x3ObjInfo
File Type:	data
Stream Size:	6
Entropy:	1.2516291673878228
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	00 00 03 00 0d 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
35.186.245.55192.168.2.22443491762025010 08/18/22-04:23:24.931708	TCP	2025010	ET TROJAN Powershell commands sent B64 1	443	49176	35.186.245.55	192.168.2.22
35.186.245.55192.168.2.22443491812025010 08/18/22-04:23:28.806682	TCP	2025010	ET TROJAN Powershell commands sent B64 1	443	49181	35.186.245.55	192.168.2.22

Network Port Distribution



Total Packets: 59

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 04:23:06.193463087 CEST	49173	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:06.193548918 CEST	443	49173	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:06.193672895 CEST	49173	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:06.207406998 CEST	49173	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:06.207438946 CEST	443	49173	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:06.380359888 CEST	443	49173	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:06.380518913 CEST	49173	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:06.391787052 CEST	49173	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:06.391815901 CEST	443	49173	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:06.392262936 CEST	443	49173	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:06.392323017 CEST	49173	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:06.842437029 CEST	49173	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:06.883389950 CEST	443	49173	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:07.087683916 CEST	443	49173	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:07.087789059 CEST	443	49173	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:07.087824106 CEST	49173	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:07.090807915 CEST	49173	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:07.103862047 CEST	49173	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:07.103905916 CEST	443	49173	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:07.103915930 CEST	49173	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:07.103952885 CEST	49173	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:19.050564051 CEST	49174	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:19.050672054 CEST	443	49174	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:19.050815105 CEST	49174	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:19.051099062 CEST	49174	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:19.051130056 CEST	443	49174	34.149.204.188	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 04:23:19.212224960 CEST	443	49174	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:19.212358952 CEST	49174	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:19.222294092 CEST	49174	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:19.222328901 CEST	443	49174	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:19.222820044 CEST	443	49174	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:19.245089054 CEST	49174	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:19.291367054 CEST	443	49174	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:19.499521971 CEST	443	49174	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:19.499900103 CEST	49174	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:19.499938011 CEST	443	49174	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:19.499965906 CEST	49174	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:19.499972105 CEST	443	49174	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:19.500001907 CEST	443	49174	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:23.998555899 CEST	49175	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:23.998600960 CEST	443	49175	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:23.998675108 CEST	49175	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:23.999838114 CEST	49175	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:23.999859095 CEST	443	49175	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:24.163655043 CEST	443	49175	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:24.163757086 CEST	49175	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:24.169996977 CEST	49175	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:24.170021057 CEST	443	49175	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:24.170578957 CEST	443	49175	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:24.209079981 CEST	49175	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:24.255384922 CEST	443	49175	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:24.468491077 CEST	443	49175	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:24.468570948 CEST	443	49175	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:24.468777895 CEST	49175	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:24.469403028 CEST	49175	443	192.168.2.22	34.149.204.188
Aug 18, 2022 04:23:24.469420910 CEST	443	49175	34.149.204.188	192.168.2.22
Aug 18, 2022 04:23:24.496511936 CEST	49176	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:24.496556044 CEST	443	49176	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:24.496635914 CEST	49176	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:24.496906042 CEST	49176	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:24.496921062 CEST	443	49176	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:24.656685114 CEST	443	49176	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:24.656788111 CEST	49176	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:24.664288998 CEST	49176	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:24.664318085 CEST	443	49176	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:24.667854071 CEST	49176	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:24.667876959 CEST	443	49176	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:24.921617985 CEST	443	49176	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:24.921694994 CEST	443	49176	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:24.921843052 CEST	49176	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:24.921859026 CEST	443	49176	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:24.921871901 CEST	49176	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:24.921907902 CEST	49176	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:24.931603909 CEST	443	49176	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:24.931698084 CEST	443	49176	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:24.931782007 CEST	443	49176	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:24.931821108 CEST	49176	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:24.931837082 CEST	49176	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:24.932337999 CEST	49176	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:24.932358980 CEST	443	49176	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:26.210772991 CEST	49177	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:26.210839987 CEST	443	49177	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:26.210918903 CEST	49177	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:26.211433887 CEST	49177	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:26.211458921 CEST	443	49177	35.186.245.55	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 04:23:26.373008013 CEST	443	49177	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:26.373100042 CEST	49177	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:26.381207943 CEST	49177	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:26.381238937 CEST	443	49177	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:26.384861946 CEST	49177	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:26.384892941 CEST	443	49177	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:26.612524986 CEST	443	49177	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:26.612626076 CEST	443	49177	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:26.612701893 CEST	49177	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:26.612737894 CEST	49177	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:26.614072084 CEST	49177	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:26.614108086 CEST	443	49177	35.186.245.55	192.168.2.22
Aug 18, 2022 04:23:26.614263058 CEST	49177	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:26.614304066 CEST	49177	443	192.168.2.22	35.186.245.55
Aug 18, 2022 04:23:26.858321905 CEST	49178	443	192.168.2.22	35.186.245.55

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 18, 2022 04:23:06.071744919 CEST	55868	53	192.168.2.22	8.8.8.8
Aug 18, 2022 04:23:06.182066917 CEST	53	55868	8.8.8.8	192.168.2.22
Aug 18, 2022 04:23:18.824484110 CEST	49688	53	192.168.2.22	8.8.8.8
Aug 18, 2022 04:23:18.931935072 CEST	53	49688	8.8.8.8	192.168.2.22
Aug 18, 2022 04:23:18.939836979 CEST	58836	53	192.168.2.22	8.8.8.8
Aug 18, 2022 04:23:19.049377918 CEST	53	58836	8.8.8.8	192.168.2.22
Aug 18, 2022 04:23:23.852726936 CEST	50134	53	192.168.2.22	8.8.8.8
Aug 18, 2022 04:23:23.871582985 CEST	53	50134	8.8.8.8	192.168.2.22
Aug 18, 2022 04:23:23.885284901 CEST	55275	53	192.168.2.22	8.8.8.8
Aug 18, 2022 04:23:23.994752884 CEST	53	55275	8.8.8.8	192.168.2.22
Aug 18, 2022 04:23:27.740761995 CEST	59915	53	192.168.2.22	8.8.8.8
Aug 18, 2022 04:23:27.850553036 CEST	53	59915	8.8.8.8	192.168.2.22
Aug 18, 2022 04:23:27.853646040 CEST	54408	53	192.168.2.22	8.8.8.8
Aug 18, 2022 04:23:27.959486961 CEST	53	54408	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 18, 2022 04:23:06.071744919 CEST	192.168.2.22	8.8.8.8	0xeea0	Standard query (0)	dullghostwhitetwintext.karewen.repl.co	A (IP address)	IN (0x0001)
Aug 18, 2022 04:23:18.824484110 CEST	192.168.2.22	8.8.8.8	0x5748	Standard query (0)	dullghostwhitetwintext.karewen.repl.co	A (IP address)	IN (0x0001)
Aug 18, 2022 04:23:18.939836979 CEST	192.168.2.22	8.8.8.8	0x5dea	Standard query (0)	dullghostwhitetwintext.karewen.repl.co	A (IP address)	IN (0x0001)
Aug 18, 2022 04:23:23.852726936 CEST	192.168.2.22	8.8.8.8	0xdc64	Standard query (0)	dullghostwhitetwintext.karewen.repl.co	A (IP address)	IN (0x0001)
Aug 18, 2022 04:23:23.885284901 CEST	192.168.2.22	8.8.8.8	0xbe50	Standard query (0)	dullghostwhitetwintext.karewen.repl.co	A (IP address)	IN (0x0001)
Aug 18, 2022 04:23:27.740761995 CEST	192.168.2.22	8.8.8.8	0x10d3	Standard query (0)	dullghostwhitetwintext.karewen.repl.co	A (IP address)	IN (0x0001)
Aug 18, 2022 04:23:27.853646040 CEST	192.168.2.22	8.8.8.8	0x722d	Standard query (0)	dullghostwhitetwintext.karewen.repl.co	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 18, 2022 04:23:06.182066917 CEST	8.8.8.8	192.168.2.22	0xeea0	No error (0)	dullghostwhitetwintext.karewen.repl.co		35.186.245.55	A (IP address)	IN (0x0001)
Aug 18, 2022 04:23:18.931935072 CEST	8.8.8.8	192.168.2.22	0x5748	No error (0)	dullghostwhitetwintext.karewen.repl.co		34.149.204.188	A (IP address)	IN (0x0001)
Aug 18, 2022 04:23:19.049377918 CEST	8.8.8.8	192.168.2.22	0x5dea	No error (0)	dullghostwhitetwintext.karewen.repl.co		34.149.204.188	A (IP address)	IN (0x0001)
Aug 18, 2022 04:23:23.871582985 CEST	8.8.8.8	192.168.2.22	0xdc64	No error (0)	dullghostwhitetwintext.karewen.repl.co		34.149.204.188	A (IP address)	IN (0x0001)
Aug 18, 2022 04:23:23.994752884 CEST	8.8.8.8	192.168.2.22	0xbe50	No error (0)	dullghostwhitetwintext.karewen.repl.co		34.149.204.188	A (IP address)	IN (0x0001)
Aug 18, 2022 04:23:27.850553036 CEST	8.8.8.8	192.168.2.22	0x10d3	No error (0)	dullghostwhitetwintext.karewen.repl.co		34.149.204.188	A (IP address)	IN (0x0001)
Aug 18, 2022 04:23:27.959486961 CEST	8.8.8.8	192.168.2.22	0x722d	No error (0)	dullghostwhitetwintext.karewen.repl.co		35.186.245.55	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- dullghostwhitetwintext.karewen.repl.co

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	35.186.245.55	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:23:06 UTC	0	OUT	OPTIONS / HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: dullghostwhitetwintext.karewen.repl.co Content-Length: 0 Connection: Keep-Alive
2022-08-18 02:23:07 UTC	0	IN	HTTP/1.1 404 Not Found Content-Length: 207 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:23:07 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7758095; includeSubDomains Connection: close
2022-08-18 02:23:07 UTC	0	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 65 20 73 65 72 76 65 72 2e 20 49 66 20 79 6f 75 20 65 6e 74 65 72 65 64 20 74 68 65 20 55 52 4c 20 6d 61 6e 75 61 6c 6c 79 20 70 6c 65 61 73 65 20 63 68 65 63 6b 20 79 6f 75 72 20 73 70 65 6c 6c 69 6e 67 20 61 6e 64 20 74 72 79 20 61 67 61 69 6e 2e 3c 2f 70 3e 0a Data Ascii: <!doctype html><html lang=en><title>404 Not Found</title> Not Found The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49174	34.149.204.188	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:23:19 UTC	0	OUT	HEAD /index.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: dullghostwhitetwintext.karewen.repl.co
2022-08-18 02:23:19 UTC	0	IN	HTTP/1.1 200 OK Content-Length: 5901 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:23:19 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7758082; includeSubDomains Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49183	35.186.245.55	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:23:29 UTC	17	OUT	HEAD /index.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: dullghostwhitetwintext.karewen.repl.co Content-Length: 0 Connection: Keep-Alive
2022-08-18 02:23:29 UTC	18	IN	HTTP/1.1 200 OK Content-Length: 5901 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:23:29 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7758072; includeSubDomains Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49175	34.149.204.188	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:23:24 UTC	1	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: dullghostwhitetwintext.karewen.repl.co
2022-08-18 02:23:24 UTC	1	IN	HTTP/1.1 404 Not Found Content-Length: 207 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:23:24 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7758077; includeSubDomains Connection: close
2022-08-18 02:23:24 UTC	1	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 65 20 73 65 72 76 65 72 2e 20 49 66 20 79 6f 75 20 65 6e 74 65 72 65 64 20 74 68 65 20 55 52 4c 20 6d 61 6e 75 61 6c 6c 79 20 70 6c 65 61 73 65 20 63 68 65 63 6b 20 79 6f 75 72 20 73 70 65 6c 6c 69 6e 67 20 61 6e 64 20 74 72 79 20 61 67 61 69 6e 2e 3c 2f 70 3e 0a Data Ascii: <!doctype html><html lang=en><title>404 Not Found</title> Not Found The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49176	35.186.245.55	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:23:24 UTC	2	OUT	GET /index.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: dullghostwhitetwintext.karewen.repl.co Connection: Keep-Alive
2022-08-18 02:23:24 UTC	2	IN	HTTP/1.1 200 OK Content-Length: 5901 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:23:24 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7758077; includeSubDomains Connection: close
2022-08-18 02:23:24 UTC	2	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 0a 47 6f 6f 64 20 74 68 69 6e 67 20 77 65 20 64 69 73 61 62 6c 65 64 20 6d 61 63 72 6f 73 0a 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 70 3e 0a 4c 6f 72 65 6d 20 69 70 73 75 6d 20 64 6f 6c 6f 72 20 73 69 74 20 61 6d 65 74 2c 20 63 6f 6e 73 65 63 74 65 74 75 72 20 61 64 69 70 69 73 63 69 6e 67 20 65 6c 69 74 2e 20 51 75 69 73 71 75 65 20 70 65 6c 6c 65 6e 74 65 73 71 75 65 20 65 67 65 73 74 61 73 20 6e 75 6c 6c 61 20 69 6e 20 64 69 67 6e 69 73 73 69 6d 2e 20 4e 61 6d 20 69 64 20 6d 61 75 72 69 73 20 6c 6f 72 65 6d 2e 20 4e 75 6e 63 20 73 75 73 63 69 70 69 74 20 69 64 20 6d 61 67 6e 61 Data Ascii: <!doctype html><html lang="en"><head><title>Good thing we disabled macros</title></head><body><p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna
2022-08-18 02:23:24 UTC	3	IN	Data Raw: 2c 20 73 65 6d 70 65 72 20 74 75 72 70 69 73 20 75 74 2c 20 67 72 61 76 69 64 61 20 6c 6f 72 65 6d 2e 20 50 72 6f 69 6e 20 61 72 63 75 20 6c 69 67 75 6c 61 2c 20 76 65 6e 65 6e 61 74 69 73 20 61 6c 69 71 75 61 6d 20 74 72 69 73 74 69 71 75 65 20 75 74 2c 20 70 72 65 74 69 75 6d 20 71 75 69 73 20 76 65 6c 69 74 2e 0a 0a 50 68 61 73 65 6c 6c 75 73 20 74 72 69 73 74 69 71 75 65 20 6f 72 63 69 20 65 6e 69 6d 2c 20 61 74 20 61 63 63 75 6d 73 61 6e 20 76 65 6c 69 74 20 69 6e 74 65 72 64 75 6d 20 65 74 2e 20 41 65 6e 65 61 6e 20 6e 65 63 20 74 72 69 73 74 69 71 75 65 20 61 6e 74 65 2c 20 64 69 67 6e 69 73 73 69 6d 20 63 6f 6e 76 61 6c 6c 69 73 20 6c 69 67 75 6c 61 2e 20 41 65 6e 65 61 6e 20 71 75 69 73 20 66 65 6c 69 73 20 64 6f 6c 6f 72 2e 20 49 6e 20 71 75 69 Data Ascii: , semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique ante, dignissim convallis ligula. Aenean quis felis dolor. In qui
2022-08-18 02:23:24 UTC	5	IN	Data Raw: 73 2c 20 74 75 72 70 69 73 20 64 6f 6c 6f 72 20 65 6c 65 69 66 65 6e 64 20 6d 61 73 73 61 2c 20 69 6e 20 6d 61 78 69 6d 75 73 20 73 61 70 69 65 6e 20 64 75 69 20 65 74 20 74 6f 72 74 6f 72 2e 20 51 75 69 73 71 75 65 20 76 61 72 69 75 73 20 65 6e 69 6d 20 73 65 64 20 65 6e 69 6d 20 76 65 6e 65 6e 61 74 69 73 20 74 65 6d 70 6f 72 2e 20 50 72 61 65 73 65 6e 74 20 71 75 69 73 20 76 6f 6c 75 74 70 61 74 20 6c 6f 72 65 6d 2e 20 50 65 6c 6c 65 6e 74 65 73 71 75 65 20 61 63 20 76 65 6e 65 6e 61 74 69 73 20 6c 61 63 75 73 2c 20 76 69 74 61 65 20 63 6f 6d 6d 6f 64 6f 20 6f 64 69 6f 2e 20 53 65 64 20 69 6e 20 6d 65 74 75 73 20 61 74 20 6c 69 62 65 72 6f 20 76 69 76 65 72 72 61 20 6d 6f 6c 6c 69 73 20 73 65 64 20 76 69 74 61 65 20 6e 69 62 68 2e 20 53 65 64 20 61 74 Data Ascii: s, turpis dolor eleifend massa, in maximus sapien dui et tortor. Quisque varius enim sed enim venenatis tempor. Praesent quis volutpat lorem. Pellentesque ac venenatis lacus, vitae commodo odio. Sed in metus at libero viverra mollis sed vitae nibh. Sed at
2022-08-18 02:23:24 UTC	6	IN	Data Raw: 20 71 75 69 73 20 65 6c 65 69 66 65 6e 64 20 6e 65 63 2c 20 73 75 73 63 69 70 69 74 20 73 69 74 20 61 6d 65 74 20 6d 61 73 73 61 2e 20 56 69 76 61 6d 75 73 20 69 6e 20 6c 65 63 74 75 73 20 65 72 61 74 2e 20 4e 75 6c 6c 61 20 66 61 63 69 6c 69 73 69 2e 20 56 69 76 61 6d 75 73 20 73 65 64 20 6d 61 73 73 61 20 71 75 69 73 20 61 72 63 75 20 65 67 65 73 74 61 73 20 76 65 68 69 63 75 6c 61 2e 20 4e 75 6c 6c 61 20 6d 61 73 73 61 20 6c 6f 72 65 6d 2c 20 74 69 6e 63 69 64 75 6e 74 20 73 65 64 20 66 65 75 67 69 61 74 20 71 75 69 73 2c 20 66 61 75 63 69 62 75 73 20 61 20 72 69 73 75 73 2e 20 53 65 64 20 76 69 76 65 72 72 61 20 74 75 72 70 69 73 20 73 69 74 20 61 6d 65 74 20 6d 65 74 75 73 20 69 61 63 75 6c 69 73 20 66 69 6e 69 62 75 73 2e 0a 0a 4d 6f 72 62 69 20 63 Data Ascii: quis eleifend nec, suscipit sit amet massa. Vivamus in lectus erat. Nulla facilisi. Vivamus sed massa quis arcu egestas vehicula. Nulla massa lorem, tincidunt sed feugiat quis, faucibus a risus. Sed viverra turpis sit amet metus iaculis finibus.Morbi c

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49177	35.186.245.55	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:23:26 UTC	8	OUT	HEAD /index.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: dullghostwhitetwintext.karewen.repl.co Content-Length: 0 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:23:26 UTC	8	IN	HTTP/1.1 200 OK Content-Length: 5901 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:23:26 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7758075; includeSubDomains Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49178	35.186.245.55	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:23:27 UTC	9	OUT	HEAD /index.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: dullghostwhitetwintext.karewen.repl.co Content-Length: 0 Connection: Keep-Alive
2022-08-18 02:23:27 UTC	9	IN	HTTP/1.1 200 OK Content-Length: 5901 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:23:27 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7758074; includeSubDomains Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49179	35.186.245.55	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:23:27 UTC	9	OUT	OPTIONS / HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: dullghostwhitetwintext.karewen.repl.co Content-Length: 0 Connection: Keep-Alive
2022-08-18 02:23:27 UTC	9	IN	HTTP/1.1 404 Not Found Content-Length: 207 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:23:27 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7758074; includeSubDomains Connection: close
2022-08-18 02:23:27 UTC	10	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 65 20 73 65 72 76 65 72 2e 20 49 66 20 79 6f 75 20 65 6e 74 65 72 65 64 20 74 68 65 20 55 52 4c 20 6d 61 6e 75 61 6c 6c 79 20 70 6c 65 61 73 65 20 63 68 65 63 6b 20 79 6f 75 72 20 73 70 65 6c 6c 69 6e 67 20 61 6e 64 20 74 72 79 20 61 67 61 69 6e 2e 3c 2f 70 3e 0a Data Ascii: <!doctype html><html lang=en><title>404 Not Found</title> Not Found The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49180	34.149.204.188	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:23:28 UTC	10	OUT	HEAD /index.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: dullghostwhitetwintext.karewen.repl.co
2022-08-18 02:23:28 UTC	10	IN	HTTP/1.1 200 OK Content-Length: 5901 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:23:28 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7758073; includeSubDomains Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49181	35.186.245.55	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:23:28 UTC	10	OUT	GET /index.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: dullghostwhitetwintext.karewen.repl.co Connection: Keep-Alive
2022-08-18 02:23:28 UTC	11	IN	HTTP/1.1 200 OK Content-Length: 5901 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:23:28 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7758073; includeSubDomains Connection: close
2022-08-18 02:23:28 UTC	11	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 0a 47 6f 6f 64 20 74 68 69 6e 67 20 77 65 20 64 69 73 61 62 6c 65 64 20 6d 61 63 72 6f 73 0a 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 70 3e 0a 4c 6f 72 65 6d 20 69 70 73 75 6d 20 64 6f 6c 6f 72 20 73 69 74 20 61 6d 65 74 2c 20 63 6f 6e 73 65 63 74 65 74 75 72 20 61 64 69 70 69 73 63 69 6e 67 20 65 6c 69 74 2e 20 51 75 69 73 71 75 65 20 70 65 6c 6c 65 6e 74 65 73 71 75 65 20 65 67 65 73 74 61 73 20 6e 75 6c 6c 61 20 69 6e 20 64 69 67 6e 69 73 73 69 6d 2e 20 4e 61 6d 20 69 64 20 6d 61 75 72 69 73 20 6c 6f 72 65 6d 2e 20 4e 75 6e 63 20 73 75 73 63 69 70 69 74 20 69 64 20 6d 61 67 6e 61 Data Ascii: <!doctype html><html lang="en"><head><title>Good thing we disabled macros</title></head><body><p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna
2022-08-18 02:23:28 UTC	12	IN	Data Raw: 2c 20 73 65 6d 70 65 72 20 74 75 72 70 69 73 20 75 74 2c 20 67 72 61 76 69 64 61 20 6c 6f 72 65 6d 2e 20 50 72 6f 69 6e 20 61 72 63 75 20 6c 69 67 75 6c 61 2c 20 76 65 6e 65 6e 61 74 69 73 20 61 6c 69 71 75 61 6d 20 74 72 69 73 74 69 71 75 65 20 75 74 2c 20 70 72 65 74 69 75 6d 20 71 75 69 73 20 76 65 6c 69 74 2e 0a 0a 50 68 61 73 65 6c 6c 75 73 20 74 72 69 73 74 69 71 75 65 20 6f 72 63 69 20 65 6e 69 6d 2c 20 61 74 20 61 63 63 75 6d 73 61 6e 20 76 65 6c 69 74 20 69 6e 74 65 72 64 75 6d 20 65 74 2e 20 41 65 6e 65 61 6e 20 6e 65 63 20 74 72 69 73 74 69 71 75 65 20 61 6e 74 65 2c 20 64 69 67 6e 69 73 73 69 6d 20 63 6f 6e 76 61 6c 6c 69 73 20 6c 69 67 75 6c 61 2e 20 41 65 6e 65 61 6e 20 71 75 69 73 20 66 65 6c 69 73 20 64 6f 6c 6f 72 2e 20 49 6e 20 71 75 69 Data Ascii: , semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique ante, dignissim convallis ligula. Aenean quis felis dolor. In qui
2022-08-18 02:23:28 UTC	14	IN	Data Raw: 73 2c 20 74 75 72 70 69 73 20 64 6f 6c 6f 72 20 65 6c 65 69 66 65 6e 64 20 6d 61 73 73 61 2c 20 69 6e 20 6d 61 78 69 6d 75 73 20 73 61 70 69 65 6e 20 64 75 69 20 65 74 20 74 6f 72 74 6f 72 2e 20 51 75 69 73 71 75 65 20 76 61 72 69 75 73 20 65 6e 69 6d 20 73 65 64 20 65 6e 69 6d 20 76 65 6e 65 6e 61 74 69 73 20 74 65 6d 70 6f 72 2e 20 50 72 61 65 73 65 6e 74 20 71 75 69 73 20 76 6f 6c 75 74 70 61 74 20 6c 6f 72 65 6d 2e 20 50 65 6c 6c 65 6e 74 65 73 71 75 65 20 61 63 20 76 65 6e 65 6e 61 74 69 73 20 6c 61 63 75 73 2c 20 76 69 74 61 65 20 63 6f 6d 6d 6f 64 6f 20 6f 64 69 6f 2e 20 53 65 64 20 69 6e 20 6d 65 74 75 73 20 61 74 20 6c 69 62 65 72 6f 20 76 69 76 65 72 72 61 20 6d 6f 6c 6c 69 73 20 73 65 64 20 76 69 74 61 65 20 6e 69 62 68 2e 20 53 65 64 20 61 74 Data Ascii: s, turpis dolor eleifend massa, in maximus sapien dui et tortor. Quisque varius enim sed enim venenatis tempor. Praesent quis volutpat lorem. Pellentesque ac venenatis lacus, vitae commodo odio. Sed in metus at libero viverra mollis sed vitae nibh. Sed at
2022-08-18 02:23:28 UTC	15	IN	Data Raw: 20 71 75 69 73 20 65 6c 65 69 66 65 6e 64 20 6e 65 63 2c 20 73 75 73 63 69 70 69 74 20 73 69 74 20 61 6d 65 74 20 6d 61 73 73 61 2e 20 56 69 76 61 6d 75 73 20 69 6e 20 6c 65 63 74 75 73 20 65 72 61 74 2e 20 4e 75 6c 6c 61 20 66 61 63 69 6c 69 73 69 2e 20 56 69 76 61 6d 75 73 20 73 65 64 20 6d 61 73 73 61 20 71 75 69 73 20 61 72 63 75 20 65 67 65 73 74 61 73 20 76 65 68 69 63 75 6c 61 2e 20 4e 75 6c 6c 61 20 6d 61 73 73 61 20 6c 6f 72 65 6d 2c 20 74 69 6e 63 69 64 75 6e 74 20 73 65 64 20 66 65 75 67 69 61 74 20 71 75 69 73 2c 20 66 61 75 63 69 62 75 73 20 61 20 72 69 73 75 73 2e 20 53 65 64 20 76 69 76 65 72 72 61 20 74 75 72 70 69 73 20 73 69 74 20 61 6d 65 74 20 6d 65 74 75 73 20 69 61 63 75 6c 69 73 20 66 69 6e 69 62 75 73 2e 0a 0a 4d 6f 72 62 69 20 63 Data Ascii: quis eleifend nec, suscipit sit amet massa. Vivamus in lectus erat. Nulla facilisi. Vivamus sed massa quis arcu egestas vehicula. Nulla massa lorem, tincidunt sed feugiat quis, faucibus a risus. Sed viverra turpis sit amet metus iaculis finibus.Morbi c

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49182	35.186.245.55	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-18 02:23:29 UTC	17	OUT	HEAD /index.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: dullghostwhitetwintext.karewen.repl.co Content-Length: 0 Connection: Keep-Alive
2022-08-18 02:23:29 UTC	17	IN	HTTP/1.1 200 OK Content-Length: 5901 Content-Type: text/html; charset=utf-8 Date: Thu, 18 Aug 2022 02:23:29 GMT Expect-Ct: max-age=2592000, report-uri="https://sentry.repl.it/api/10/security/?sentry_key=615192fd532445bfbbbe966cd7131791" Replit-Cluster: global Server: Werkzeug/2.1.2 Python/3.8.12 Strict-Transport-Security: max-age=7758072; includeSubDomains Connection: close

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: **2960**, Parent PID: **576**

General

Target ID:	0
Start time:	04:22:15
Start date:	18/08/2022
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:	0x13fd60000
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	7FEE908F645	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE907DBCD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FEE908B1C3	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	7FEE907DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE907DBCD	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	7FEE908F645	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE907DBCD	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	7FEE908B1C3	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	7FEE907DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE907DBCD	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	6E1D2B14	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	7FEE9074B20	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	success or wait	1	7FEE908AD42	DeleteFileW
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	success or wait	1	7FEE908AD42	DeleteFileW
C:\Users\user\Desktop\~$ZGt61uGv.docx	success or wait	1	6E250648	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\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 6b 39 6c 6e 1e fd fd 48 fd fd fd 4a fd fd 2f 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 66 5d 2c fd fd fd 16 48 fd 5e fd fd fd 36 03 fd 05 00 00 00 00 00 00 00 fd 2b 39 fd 03 2e 06 44 fd fd 72 17 eb 30 fd 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 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	MeFyzk9lnHJ/S,XFFaqf],H^6+9.Dr0xxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	76	40	66 5d 2c fd fd fd 16 48 fd 5e fd fd fd 36 03 fd 05 00 00 00 00 00 00 00 fd 2b 39 fd 03 2e 06 44 fd fd 72 17 eb 30 fd	f],H^6+9.Dr0	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	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	zV @	success or wait	2	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	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	zV @	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 6b 39 6c 6e 1e fd fd 48 fd fd fd 4a fd fd 2f 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 66 5d 2c fd fd fd 16 48 fd 5e fd fd fd 36 03 fd 05 00 00 00 00 00 00 00 fd 2b 39 fd 03 2e 06 44 fd fd 72 17 eb 30 fd 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	MeFyzk9lnHJ/S,XFFaqf],H^6+9.Dr0xxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	76	40	66 5d 2c fd fd fd 16 48 fd 5e fd fd fd 36 03 fd 05 00 00 00 00 00 00 00 fd 2b 39 fd 03 2e 06 44 fd fd 72 17 eb 30 fd	f],H^6+9.Dr0	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	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	zV	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	2576	4	03 10 fd fd		success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 6b 39 6c 6e 1e fd fd 48 fd fd fd 4a fd fd 2f 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 66 5d 2c fd fd fd 16 48 fd 5e fd fd fd 36 03 fd 05 00 00 00 00 00 00 00 fd 2b 39 fd 03 2e 06 44 fd fd 72 17 eb 30 fd 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	MeFyzk9lnHJ/S,XFFaqf], H^6+9.Dr0xxxx	success or wait	1	7FEE9047A59	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 6b 39 6c 6e 1e fd fd 48 fd fd fd 4a fd fd 2f 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 0e 21 fd 29 3b fd 4e fd 1b fd 3f 13 fd fd 4c 0b 00 00 00 00 00 00 00 fd 2b 39 fd 03 2e 06 44 fd fd 72 17 eb 30 fd 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	MeFyzk9lnHJ/S,XFFaq!);N?L+9.Dr0AExxxx	success or wait	2	7FEE908B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	fd 0e 21 fd 29 3b fd 4e fd 1b fd 3f 13 fd fd 4c 0b 00 00 00 00 00 00 00 fd 2b 39 fd 03 2e 06 44 fd fd 72 17 eb 30 fd	!);N?L+9.Dr0	success or wait	1	7FEE9047A59	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 fd 0f fd fd fd 4a fd fd fd fd 33 fd 07 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ J3>I	success or wait	1	7FEE9047A59	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 fd 47 27 0b 34 fd 2d 4e fd fd 57 47 3d fd 26 49 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 60 fd 6a 1f 38 51 fd 4d fd fd 25 fd fd fd 4d 52 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 36 2b fd 44 fd fd 42 20 fd 5b 5b 6f 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 6f 5a fd fd fd 40 fd 41 fd fd fd fd 49 2e 38 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 fd fd 5e 70 00 fd fd 48 fd e3 fd 3d fd 33 fd 01 00 00 00 14 00 00	zVG'4-NWG=&I;efHkX,`j8QM%MR;efHkX,+DB[[o;efHkX,oZ@AI.8;efHkX,^pH=3	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	2580	50	05 fd 00 fd 40 03 07 fd 47 27 0b 34 fd 2d 4e fd fd 57 47 3d fd 26 49 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	@G'4-NWG=&I	success or wait	3	7FEE9047A59	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	7FEE9047A59	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 6b 39 6c 6e 1e fd fd 48 fd fd fd 4a fd fd 2f 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 0e 21 fd 29 3b fd 4e fd 1b fd 3f 13 fd fd 4c 0b 00 00 00 00 00 00 00 00 fd 2b 39 fd 03 2e 06 44 fd fd 72 17 eb 30 fd 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	MeFyzk9lnHJ/S,XFFaq!); N?L+9.Dr0AExxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	fd 0e 21 fd 29 3b fd 4e fd 1b fd 3f 13 fd fd 4c 0b 00 00 00 00 00 00 00 fd 2b 39 fd 03 2e 06 44 fd fd 72 17 eb 30 fd	!);N?L+9.Dr0	success or wait	1	7FEE9047A59	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 3c 4c fd fd 5f fd 6c 44 fd 07 05 0a fd 25 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 5d fd 78 25 74 fd fd 45 fd 0c fd 44 fd 44 fd 01 00 00 00 11 00 00 00 00 00 00 00 fd 6a fd fd 6d fd 5e 4f fd 7b 48 08 55 fd fd fd 01 00 00 00 06 20 fd fd 7f fd fd fd fd 5d fd 4d fd 17 7f 32 fd 51 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 fd 1f 05 fd 67 fd fd 4d fd 0e fd 70 17 fd 09 7f 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	zV<L_lD0MMCOYpe]x%t EDDjm^O{HU]M2QJRwpsgMp	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	14904	122	ea 69 49 00 0c 56 0c 3c 4c fd fd 5f fd 6c 44 fd 07 05 0a fd 25 fd fd 17 1f fd fd 54 fd 44 fd ab fd fd 58 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 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 1f 05 fd 67 fd fd 4d fd 0e fd 70 17 fd 09 7f 05	iIV<L_lDTDX` 8fJRwpsJRwpsgMp	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	10824	56	03 10 fd fd 06 00 fd 3c 4c fd fd 5f fd 6c 44 fd 07 05 0a fd 25 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	<L_lD0MMCOYpe	success or wait	4	7FEE9047A59	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	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	7FEE9047A59	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 6b 39 6c 6e 1e fd fd 48 fd fd fd 4a fd fd 2f 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 0e 21 fd 29 3b fd 4e fd 1b fd 3f 13 fd fd 4c 0b 00 00 00 00 00 00 00 fd 2b 39 fd 03 2e 06 44 fd fd 72 17 eb 30 fd 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	MeFyzk9lnHJ/S,XFFaq!);N?L+9.Dr0AExxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	fd 0e 21 fd 29 3b fd 4e fd 1b fd 3f 13 fd fd 4c 0b 00 00 00 00 00 00 00 fd 2b 39 fd 03 2e 06 44 fd fd 72 17 eb 30 fd	!);N?L+9.Dr0	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15208	134	ea 69 49 00 0c 56 0c 7f fd fd fd fd 5d fd 4d fd 17 7f 32 fd 51 fd fd fd fd 29 2e 6f 48 fd fd fd 7d fd 3d fd fd 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd fd fd fd 32 fd 13 4e fd fd fd 22 fd fd fd fd 01 00 00 11 03 39 03 00 75 fd 00 fd 60 03 0c 25 2a fd fd 38 fd fd 47 fd fd fd 04 63 78 35 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	iIV]M2Q).oH}=22N"9u`%*8Gcx59,'Ma6)X>y	success or wait	4	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15720	70	ea 69 49 00 0c 56 34 7f fd fd fd fd 5d fd 4d fd 17 7f 32 fd 51 fd fd fd fd 29 2e 6f 48 fd fd fd 7d fd 3d fd fd 0a 00 00 00 00 00 00 00 07 58 22 0c fd 6a fd fd 6d fd 5e 4f fd 7b 48 08 55 fd fd fd 05	iIV4]M2Q).oH}=X"jm^O{HU	success or wait	4	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-CNRY.FSD	2804	448	05 fd 00 fd 6d 07 11 7f fd fd fd fd 5d fd 4d fd 17 7f 32 fd 51 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 7f fd fd fd 5d fd 4d fd 17 7f 32 fd 51 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 7f fd fd fd fd 5d fd 4d fd 17 7f 32 fd 51 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 7f fd fd fd fd 5d fd 4d fd 17 7f 32 fd 51 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 7f fd fd fd fd 5d fd 4d fd 17 7f 32 fd 51 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	m]M2Q~]M2Q]M2Q]M2Q]M2Q	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 6b 39 6c 6e 1e fd fd 48 fd fd fd 4a fd fd 2f 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 0e 21 fd 29 3b fd 4e fd 1b fd 3f 13 fd fd 4c 0b 00 00 00 00 00 00 00 fd 2b 39 fd 03 2e 06 44 fd fd 72 17 eb 30 fd 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	MeFyzk9lnHJ/S,XFFaq!);N?L+9.Dr0AExxxx	success or wait	1	7FEE9047A59	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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSF-CTBL.FSF	16	2	0c 00		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSF-CTBL.FSF	18	1	18		success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4d fd 09 37 fd fd 2b 4d fd fd 11 fd 4c fd fd 4e 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 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12 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	MeFyzM7+MLNS,XFFaq J@BH)%5VJ SWxxxx*	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	fd 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12	J@BH)%5VJ	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4d fd 09 37 fd fd 2b 4d fd fd 11 fd 4c fd fd 4e 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 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12 00 53 00 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 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	MeFyzM7+MLNS,XFFaq J@BH)%5VJ SWxxxx*	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	fd 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12	J@BH)%5VJ	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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 6c fd fd 78 fd fd 47 fd 12 41 fd fd 2f 63 6f 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 5f fd fd fd fd fd 5f 48 fd fd 46 4a 58 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 fd fd 76 fd fd fd 42 fd 34 68 fd fd ad 09 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 3a 75 fd fd 5a 4d fd fd 59 1b 18 fd 2e fd 01 00 00 00 01 07 00 07 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 76 fd fd fd 42 fd 34 68 fd fd ad 09 01 00 00 00 05 fd 00 fd 6d 07 24 11 44 54 fd	zV@lxGA/coG__HJXWvB4hb:uZMY.`vB4hm$DT	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	2576	4	03 10 fd fd		success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4d fd 09 37 fd fd 2b 4d fd fd 11 fd 4c fd fd 4e 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 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12 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	MeFyzM7+MLNS,XFFaqJ@BH)%5VJ SWxxxx*	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4d fd 09 37 fd fd 2b 4d fd fd 11 fd 4c fd fd 4e 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 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12 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	MeFyzM7+MLNS,XFFaq J@BH)%5VJ SWxxxx*	success or wait	1	7FEE9047A59	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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	2	0c 00		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	18	2	18 fd		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	20	1	5d	]	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	21	92	46 00 53 00 44 00 2d 00 7b 00 38 00 32 00 44 00 36 00 44 00 30 00 34 00 41 00 2d 00 45 00 32 00 41 00 37 00 2d 00 34 00 32 00 46 00 31 00 2d 00 38 00 39 00 41 00 36 00 2d 00 43 00 46 00 44 00 35 00 37 00 46 00 39 00 45 00 43 00 37 00 36 00 36 00 7d 00 2e 00 46 00 53 00 44 00	FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	113	1	05		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	fd 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12	J@BH)%5VJ	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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 5e 6b fd 73 2f 65 4f fd 50 fd fd 14 78 fd fd 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ ^ks/eOPx>I	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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 6c fd fd 78 fd fd 47 fd 12 41 fd fd 2f 63 6f 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 fd fd 76 fd fd fd 42 fd 34 68 fd fd ad 09 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 3a 75 fd fd 5a 4d fd fd 59 1b 18 fd 2e 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 14 17 58 15 7c fd fd 45 fd fd 3d 38 fd fd fd 14 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 04 fd 62 fb 23 46 fd 4d 23 6e 4c 43 28 48 01 00 00 00 13 00 00	zVlxGA/co;efHkX,vB4h;efHkX,:uZ MY.;efHkX,X|E=8;efHkX, b#FM#nLC(H	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	2580	50	05 fd 00 fd 40 03 07 6c fd fd 78 fd fd 47 fd 12 41 fd fd 2f 63 6f 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	@lxGA/co	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4d fd 09 37 fd fd 2b 4d fd fd 11 fd 4c fd fd 4e 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 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12 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	MeFyzM7+MLNS,XFFaq J@BH)%5VJ SWxxxx*	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	fd 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12	J@BH)%5VJ	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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 5f fd fd fd fd fd 5f 48 fd fd 46 4a 58 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 fd fd fd 23 fd fd 49 fd fd fd 2e fd 5f 3d 01 00 00 00 10 00 00 00 00 00 00 00 0c 18 fd fd 7d fd 36 4a fd 23 fd 0f fd fd 5a fd 01 00 00 00 06 20 fd fd 11 44 54 fd fd 26 fd 45 fd fd 1e 0a fd 72 fd 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 42 52 fd fd 13 fd 4c 42 fd b1 fd 78 fd fd 79 01 00 00 00 06 00 fd fd fd fd 72 5d fd fd 42 fd 3c 00 fd 63 fd fd 3a 01 00 00 00 1c 00 00 00 00 00 00 00 96 fd fd 01 fd 40 fd fd fd 4b fd 04 1f 01 00 00 00 06 20 fd fd 29 5b fd	zV__HJX0MMCOYpeI.=}6J#Z DT&ErJ RwpsBRLBxyr]B<c:@K)[	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	14904	122	ea 69 49 01 0c 56 0c 5f fd fd fd fd fd 5f 48 fd fd 46 4a 58 fd fd fd fd fd fd fd fd fd 48 fd fd 14 fd fd 66 fd 0f 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 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 42 52 fd fd 13 fd 4c 42 fd b1 fd 78 fd fd 79 05	iIV__HJXHf` 8fJRwpsJRwpsBRLBxy	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	15032	81	3e 03 00 00 54 07 00 00 00 fd 54 27 0c 5f fd fd fd fd 5f 48 fd fd 46 4a 58 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 42 52 fd fd 13 fd 4c 42 fd b1 fd 78 fd fd 79 01 00 00 00 fd fd 01	>TT'__HJXyjXSQJRwps BRLBxy	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	10824	56	03 10 fd fd 06 00 fd 5f fd fd fd fd fd 5f 48 fd fd 46 4a 58 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 00	__HJX0MMCOYpe	success or wait	4	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4d fd 09 37 fd fd 2b 4d fd fd 11 fd 4c fd fd 4e 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 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12 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	MeFyzM7+MLNS,XFFaq J@BH)%5VJ SWxxxx*	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	fd 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12	J@BH)%5VJ	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	15208	284	ea 69 49 01 0c 56 0c 11 44 54 fd fd 26 fd 45 fd fd 1e 0a fd 72 fd fd fd fd fd fd 5f 5e fd 42 fd 4b 6a 7e fd 3e fd 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd 6d fd 36 38 fd 46 fd 42 fd fd fd fd fd 3c fd fd 01 00 00 11 03 fd 0b 00 75 fd 00 fd 00 fd 01 0b 0c d8 fd fd 7f 7c fd 46 fd 6a 20 7f 28 fd 70 77 0c fd 20 37 fd fd 70 fd 47 fd fd fd 0f fd fd 42 51 0c fd 2c 71 fd fd 1e 44 fd 46 27 fd 6f 38 fd 0c fd 4a 03 34 03 2f 4b fd 46 fd 68 18 63 fd 6f 0c 42 5e 3e 1b 62 5e 2e 4e fd 6a 6e fd 79 fd fd 09 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	iIVDT&Er_^BKj>2m68FB <u|Fj (pw 7pGBQ,DF'o8J4/KFhcoB ^>b^.Njny; zIW*dO(@9DHV0O0B5B	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	15752	70	ea 69 49 01 0c 56 2c 11 44 54 fd fd 26 fd 45 fd fd 1e 0a fd 72 fd fd fd fd fd fd 5f 5e fd 42 fd 4b 6a 7e fd 3e fd 08 00 00 00 00 00 00 00 07 58 22 0c 0c 18 fd fd 7d fd 36 4a fd 23 fd 0f fd fd 5a fd 05	iIV,DT&Er_^BKj>X"}6J#Z	success or wait	4	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	2804	398	05 fd 00 fd 6d 07 24 11 44 54 fd fd 26 fd 45 fd fd 1e 0a fd 72 fd 01 00 00 00 01 04 00 09 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 11 44 54 fd fd 26 fd 45 fd fd 1e 0a fd 72 fd 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 11 44 54 fd fd 26 fd 45 fd fd 1e 0a fd 72 fd 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 09 11 44 54 fd fd 26 fd 45 fd fd 1e 0a fd 72 fd 05 00 00 00 01 02 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 15 fd fd fd 23 fd fd 49 fd fd fd 2e fd 5f 3d 01 00 00 00 01 00 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	m$DT&ErDT&ErDT&ErDT&ErI.=	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4d fd 09 37 fd fd 2b 4d fd fd 11 fd 4c fd fd 4e 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 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12 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	MeFyzM7+MLNS,XFFaqJ@BH)%5VJ SWxxxx*	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	fd 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12	J@BH)%5VJ	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	17592	114	ea 69 49 01 0c 56 0c 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 fd fd fd fd fd 1e 50 fd 4f fd fd 7f 6a 0f 4e 34 fd 03 00 00 00 00 00 00 00 0b fd 00 fd 2a 0c d8 fd fd 7f 7c fd 46 fd 6a 20 7f 28 fd 70 77 03 19 03 00 75 fd 00 fd 40 03 0c 14 40 fd fd 18 2f fd 4c fd 4e fd fd 36 72 fd fd 00 19 01 00 00 00 00 00 00 00 50 38 00 1c 79 05	iIV)[v@o3|APOjN4*|Fj (pwu@@/LN6rP8y	success or wait	4	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	18144	70	ea 69 49 01 0c 56 34 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 fd fd fd fd fd 1e 50 fd 4f fd fd 7f 6a 0f 4e 34 fd 0a 00 00 00 00 00 00 00 07 58 22 0c 96 fd fd 01 fd 40 fd fd fd 4b fd 04 1f 05	iIV4) [v@o3|APOjN4X"@K	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	18384	555	3e 03 00 00 54 07 00 00 00 fd 54 27 14 11 44 54 fd fd 26 fd 45 fd fd 1e 0a fd 72 fd 19 00 fd 03 00 00 fd 54 27 1c 11 44 54 fd fd 26 fd 45 fd fd 1e 0a fd 72 fd 39 00 fd 03 00 00 fd 54 27 0c 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 19 00 fd 03 00 00 fd 54 27 2c 11 44 54 fd fd 26 fd 45 fd fd 1e 0a fd 72 fd 29 00 72 03 00 00 58 2b 29 0c 18 fd fd 7d fd 36 4a fd 23 fd 0f fd fd 5a fd 01 00 00 00 fd 54 27 14 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 39 00 fd 03 00 00 fd 54 fd 0c fd fd fd 72 5d fd fd 42 fd 3c 00 fd 63 fd fd 3a fd 09 0c 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 14 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 1c 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 24 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 7a 03 00	>TT'DT&ErT'DT&Er9T') [v@o3|AT', DT&Er)rX+)}6J#ZT') [v@o3|A9Tr]B<c:) [v@o3|A)[v@o3|A) [v@o3|A$)[v@o3|Az	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	3202	472	05 fd 00 fd fd 08 0f 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 01 00 00 00 01 06 00 14 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 08 11 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 02 00 00 00 01 06 00 15 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 08 15 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 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 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 04 00 00 00 01 01 00 17 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 08 09 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 06 00 00 00 01 02 00 18 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd	)[v@o3|A)[v@o3|A) [v@o3|A)[v@o3|A) [v@o3|A	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4d fd 09 37 fd fd 2b 4d fd fd 11 fd 4c fd fd 4e 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 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12 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	MeFyzM7+MLNS,XFFaqJ@BH)%5VJ SWxxxx*	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 15 11 0f 48 2a 01 4f fd b1 fd 4c fd 10 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 2f 67 3a 54 1d 43 fd 42 fd 74 15 3b fd 02 05 00 00 00 00 00 00 00 fd 06 fd 37 fd fd 42 fd 5a fd fd fd 2f 5e 54 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	MeFyzH*OLS,XFFaq/gTCBt;7BZ/^Txxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	76	40	fd 2f 67 3a 54 1d 43 fd 42 fd 74 15 3b fd 02 05 00 00 00 00 00 00 00 fd 06 fd 37 fd fd 42 fd 5a fd fd fd 2f 5e 54	/gTCBt;7BZ/^T	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	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 00 00 00	zV @	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	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	zV @	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 15 11 0f 48 2a 01 4f fd b1 fd 4c fd 10 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 2f 67 3a 54 1d 43 fd 42 fd 74 15 3b fd 02 05 00 00 00 00 00 00 00 fd 06 fd 37 fd fd 42 fd 5a fd fd fd 2f 5e 54 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	MeFyzH*OLS,XFFaq/gTCBt;7BZ/^Txxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	76	40	fd 2f 67 3a 54 1d 43 fd 42 fd 74 15 3b fd 02 05 00 00 00 00 00 00 00 fd 06 fd 37 fd fd 42 fd 5a fd fd fd 2f 5e 54	/gTCBt;7BZ/^T	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	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	zV	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	2576	4	03 10 fd fd		success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	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	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 15 11 0f 48 2a 01 4f fd b1 fd 4c fd 10 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 2f 67 3a 54 1d 43 fd 42 fd 74 15 3b fd 02 05 00 00 00 00 00 00 00 fd 06 fd 37 fd fd 42 fd 5a fd fd fd 2f 5e 54 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	MeFyzH*OLS,XFFaq/gTCBt;7BZ/^Txxxx	success or wait	1	7FEE9047A59	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 fd 15 11 0f 48 2a 01 4f fd b1 fd 4c fd 10 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 26 0c fd fd fd 46 fd 7e fd 63 fd fd fd 0b 00 00 00 00 00 00 00 fd 06 fd 37 fd fd 42 fd 5a fd fd fd 2f 5e 54 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 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	MeFyzH*OLS,XFFaq&F~c7BZ/^TAExxxx	success or wait	2	7FEE908B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	fd 26 0c fd fd fd fd 46 fd 7e fd 63 fd fd fd fd 0b 00 00 00 00 00 00 00 fd 06 fd 37 fd fd 42 fd 5a fd fd fd 2f 5e 54	&F~c7BZ/^T	success or wait	1	7FEE9047A59	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 2c fd 2d 44 10 77 3c 41 fd fd fd fd 15 06 fd 4e 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ ,-Dw<AN>I	success or wait	1	7FEE9047A59	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	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 6b 5f 3a fd 7e fd fd 40 fd 74 fd c6 fd 14 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 76 0f 64 21 42 4a fd 44 fd 46 fd 0b fd 4b fd 62 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 7d fd 57 fd fd fd 4d fd fd fd fd fd 12 61 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 4b 23 fd 2d 68 20 55 4c fd 0a 07 5f fd 27 28 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 fd fd fd 50 22 59 37 4b fd 2d 1a 52 1f c1 72 01 00 00 00 14 00 00	zVk_:~@t;efHkX,vd!BJDFKb;efHkX ,}WMa;efHkX,K#-h UL_'(;efHkX,P"Y7K-Rr	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	2580	50	05 fd 00 fd 40 03 07 6b 5f 3a fd 7e fd fd 40 fd 74 fd c6 fd 14 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	@k_:~@t	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\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	7FEE9047A59	WriteFile
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 fd 15 11 0f 48 2a 01 4f fd b1 fd 4c fd 10 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 26 0c fd fd fd fd 46 fd 7e fd 63 fd fd fd fd 0b 00 00 00 00 00 00 00 fd 06 fd 37 fd fd 42 fd 5a fd fd fd 2f 5e 54 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	MeFyzH*OLS,XFFaq&F~c7BZ/^TAExxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	fd 26 0c fd fd fd fd 46 fd 7e fd 63 fd fd fd fd 0b 00 00 00 00 00 00 00 fd 06 fd 37 fd fd 42 fd 5a fd fd fd 2f 5e 54	&F~c7BZ/^T	success or wait	1	7FEE9047A59	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 67 72 fd 4a 63 fd fd 48 fd 72 fd 0e 04 fd fd 54 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 51 fd 67 7a 23 fd 07 4b fd 1f 29 0a fd fd 35 fd 01 00 00 00 11 00 00 00 00 00 00 00 2f fd 48 fd fd fd fd 43 fd 4a fd 05 fd 5d 7b 01 00 00 00 06 20 fd fd 23 5c fd fd 62 fd fd 46 fd 07 4a fd 30 67 50 fd 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 01 71 fd fd 07 fd 5e 49 fd fd fd 55 16 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	zVgrJcHrT0MMCOYpeQgz#K)5/HCJ]{#\bFJ0gPJRwpsq^IU	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	14904	122	ea 69 49 00 0c 56 0c 67 72 fd 4a 63 fd fd 48 fd 72 fd 0e 04 fd fd 54 fd 78 0b 1a fd 61 5c 79 40 fd fd 7e 3c fd fd 5f 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 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 01 71 fd fd 07 fd 5e 49 fd fd fd 55 16 fd fd fd 05	iIVgrJcHrTxa\y@~<_`8fJRwpsJRwpsq^IU	success or wait	1	7FEE9047A59	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 67 72 fd 4a 63 fd fd 48 fd 72 fd 0e 04 fd fd 54 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 01 71 fd fd 07 fd 5e 49 fd fd fd 55 16 fd fd fd 01 00 00 00 fd fd 01	>TT'grJcHrTyjXSQJRwpsq^IU	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	10824	56	03 10 fd fd 06 00 fd 67 72 fd 4a 63 fd fd 48 fd 72 fd 0e 04 fd fd 54 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	grJcHrT0MMCOYpe	success or wait	4	7FEE9047A59	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	7FEE9047A59	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 fd 15 11 0f 48 2a 01 4f fd b1 fd 4c fd 10 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 26 0c fd fd fd fd 46 fd 7e fd 63 fd fd fd fd 0b 00 00 00 00 00 00 00 00 fd 06 fd 37 fd fd 42 fd 5a fd fd fd 2f 5e 54 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	MeFyzH*OLS,XFFaq&F~c7BZ/^TAExxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	fd 26 0c fd fd fd fd 46 fd 7e fd 63 fd fd fd fd 0b 00 00 00 00 00 00 00 fd 06 fd 37 fd fd 42 fd 5a fd fd fd 2f 5e 54	&F~c7BZ/^T	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	15208	134	ea 69 49 00 0c 56 0c 23 5c fd fd 62 fd fd 46 fd 07 4a fd 30 67 50 fd fd 0b 7f fd 01 32 75 62 45 fd fd 6f 48 27 fd 1b fd 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd fd 66 75 fd 08 01 fd 46 fd 29 7a 6a 03 6d 66 09 01 00 00 11 03 39 03 00 75 fd 00 fd 60 03 0c 13 6a 10 05 0e 12 6a 44 fd fd 5a fd 4e 47 4b 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	iIV#\bFJ0gP2ubEoH'2fuF)zjmf9u` jjDZNGK9,'Ma6)X>y	success or wait	4	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	15720	70	ea 69 49 00 0c 56 34 23 5c fd fd 62 fd fd 46 fd 07 4a fd 30 67 50 fd fd 0b 7f fd 01 32 75 62 45 fd fd 6f 48 27 fd 1b fd 0a 00 00 00 00 00 00 07 58 22 0c 2f fd 48 fd fd fd fd 43 fd 4a fd 05 fd 5d 7b 05	iIV4#\bFJ0gP2ubEoH'X"/HCJ]{	success or wait	2	7FEE9047A59	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 23 5c fd fd 62 fd fd 46 fd 07 4a fd 30 67 50 fd 29 00 72 03 00 00 58 2b 29 2f fd 48 fd fd fd fd 43 fd 4a fd 05 fd 5d 7b 01 00 00 00 fd 54 27 0c 67 72 fd 4a 63 fd fd 48 fd 72 fd 0e 04 fd fd 54 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 01 71 fd fd 07 fd 5e 49 fd fd fd 55 16 fd fd fd 01 00 00 00 fd 54 fd 0c 51 fd 67 7a 23 fd 07 4b fd 1f 29 0a fd fd 35 fd fd 09 0c 23 5c fd fd 62 fd fd 46 fd 07 4a fd 30 67 50 fd 14 23 5c fd fd 62 fd fd 46 fd 07 4a fd 30 67 50 fd 1c 23 5c fd fd 62 fd fd 46 fd 07 4a fd 30 67 50 fd 24 23 5c fd fd 62 fd fd 46 fd 07 4a fd 30 67 50 fd 7a 03 00 00 fd 54 27 0c 23 5c fd fd 62 fd fd 46 fd 07 4a fd 30 67 50 fd 39 00 fd 03 00 00 fd 54 27 14 23 5c fd fd	>TT'4#\bFJ0gP)rX+)/HCJ]{T'grJc HrTyjXSQJRwpsq^lUTQgz#K)5#\bFJ 0gP#\bFJ0gP#\bFJ0gP$ #\bFJ0gPzT '#\bFJ0gP9T'#\	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	2804	448	05 fd 00 fd 6d 07 11 23 5c fd fd 62 fd fd 46 fd 07 4a fd 30 67 50 fd 01 00 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 0f 23 5c fd fd 62 fd fd 46 fd 07 4a fd 30 67 50 fd 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 23 5c fd fd 62 fd fd 46 fd 07 4a fd 30 67 50 fd 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 11 23 5c fd fd 62 fd fd 46 fd 07 4a fd 30 67 50 fd 04 00 00 00 01 06 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 09 23 5c fd fd 62 fd fd 46 fd 07 4a fd 30 67 50 fd 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#\bFJ0gP~#\bFJ0gP#\bFJ0gP#\bF J0gP#\bFJ0gP	success or wait	3	7FEE9047A59	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	7FEE9047A59	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	7FEE9047A59	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	7FEE9047A59	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 fd 15 11 0f 48 2a 01 4f fd b1 fd 4c fd 10 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 26 0c fd fd fd fd 46 fd 7e fd 63 fd fd fd fd 0b 00 00 00 00 00 00 00 fd 06 fd 37 fd fd 42 fd 5a fd fd fd 2f 5e 54 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	MeFyzH*OLS,XFFaq&F~c7BZ/^TAExxxx	success or wait	1	7FEE9047A59	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	7FEE9047A59	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	7FEE9047A59	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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 7a 49 fd 02 fd 5a 53 62 4f fd 2a 47 0b 18 38 80 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 87 70 fd fd 46 47 fd fd fd 2b 40 fd 48 fd 0b 00 00 00 00 00 00 00 64 13 fd fd fd 24 2f 48 fd 1d fd 10 4e 0f fd 2d 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 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 00 00	MeFyzIZSbO*G8S,XFFaqpFG+@Hd$/HN-P>PBxxxx+	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	fd 87 70 fd fd 46 47 fd fd fd 2b 40 fd 48 fd 0b 00 00 00 00 00 00 00 64 13 fd fd fd 24 2f 48 fd 1d fd 10 4e 0f fd 2d	pFG+@Hd$/HN-	success or wait	1	7FEE9047A59	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-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.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	zV @pGsqQ9Ga`qbpG|u-uAW"U	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.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	zV @pGsqQ9Ga`qbpG|u-uAW"U	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 49 fd 02 fd 5a 53 62 4f fd 2a 47 0b 18 38 80 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 87 70 fd fd 46 47 fd fd fd 2b 40 fd 48 fd 0b 00 00 00 00 00 00 00 64 13 fd fd fd 24 2f 48 fd 1d fd 10 4e 0f fd 2d 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	MeFyzIZSbO*G8S,XFFaqpFG+@Hd$/HN-P>PBxxxx+	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	fd 87 70 fd fd 46 47 fd fd fd 2b 40 fd 48 fd 0b 00 00 00 00 00 00 00 64 13 fd fd fd 24 2f 48 fd 1d fd 10 4e 0f fd 2d	pFG+@Hd$/HN-	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.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 fd fd 00 fd b3 fd 43 fd fd fd 1e fd 37 fd 4c 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 23 36 12 29 fd fd 42 fd 53 65 21 0b 37 fd 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 fd fd 44 70 fd 75 fd 49 fd 08 1e fd 24 10 2e fd 01 00 00 00 01 07 00 04 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 62 07 0b 5e 42 5c 58 03 fd fd 48 fd 3b fd 4a 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 00 00 00 00 07 60 fd fd fd fd 44 70 fd 75 fd 49 fd 08 1e fd 24 10 2e fd 01 00 00 00 05 fd 00 fd 6d 07 11 fd fd 43 19	zV@C7LG#6)BSe!7WDpuI$.b^B\XH;J`DpuI$.mC	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	2576	4	03 10 fd fd		success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.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	7FEE9047A59	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-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 49 fd 02 fd 5a 53 62 4f fd 2a 47 0b 18 38 80 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 87 70 fd fd 46 47 fd fd fd 2b 40 fd 48 fd 0b 00 00 00 00 00 00 00 64 13 fd fd fd 24 2f 48 fd 1d fd 10 4e 0f fd 2d 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	MeFyzIZSbO*G8S,XFFaqpFG+@Hd$/HN-P>PBxxxx+	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 49 fd 02 fd 5a 53 62 4f fd 2a 47 0b 18 38 80 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd 87 70 fd fd 46 47 fd fd fd 2b 40 fd 48 fd 0b 00 00 00 00 00 00 00 64 13 fd fd fd 24 2f 48 fd 1d fd 10 4e 0f fd 2d 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzIZSbO*G8S,XFFaqpFG+@Hd$/HN-P>PBxxxx+	success or wait	1	7FEE9047A59	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	7FEE9047A59	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	7FEE9047A59	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	7FEE9047A59	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	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	21	92	46 00 53 00 44 00 2d 00 7b 00 45 00 43 00 41 00 46 00 36 00 46 00 46 00 33 00 2d 00 46 00 39 00 43 00 46 00 2d 00 34 00 39 00 35 00 42 00 2d 00 38 00 30 00 44 00 42 00 2d 00 38 00 30 00 33 00 35 00 44 00 45 00 41 00 33 00 30 00 39 00 45 00 37 00 7d 00 2e 00 46 00 53 00 44 00	FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	113	1	05		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	fd 87 70 fd fd 46 47 fd fd fd 2b 40 fd 48 fd 0b 00 00 00 00 00 00 00 64 13 fd fd fd 24 2f 48 fd 1d fd 10 4e 0f fd 2d	pFG+@Hd$/HN-	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	6656	51	fd 36 27 fd fd 17 41 fd fd 7b 67 06 fd 13 0d 03 00 02 00 fd 00 40 20 7c 53 13 61 fd fd fd 4d fd fd 62 fd 49 fd fd 0d 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ |SaMbI>I	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	6712	4096	fd fd fd fd fd 7a 56 fd 12 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd fd fd 00 fd b3 fd 43 fd fd fd 1e fd 37 fd 4c 01 00 00 00 02 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 01 00 00 00 06 00 fd fd fd 44 70 fd 75 fd 49 fd 08 1e fd 24 10 2e fd 01 00 00 00 05 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd 5e 42 5c 58 03 fd fd 48 fd 3b fd 4a fd fd fd fd 01 00 00 00 08 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd 51 fd fd 63 fd 07 fd 4f fd 3a fd fd fd fd 54 fd 01 00 00 00 0d 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd 50 fd 34 63 fd fd fd 4b fd fd 70 64 08 fd 6f 59 01 00 00 00 11 00 00	zVC7L;efHkX,DpuI$.;efHkX,^B\XH;J;efHkX,QcO:T;efHkX,P4cKpdoY	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	2580	50	05 fd 00 fd 40 03 07 fd fd 00 fd b3 fd 43 fd fd fd 1e fd 37 fd 4c 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	@C7L	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.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	7FEE9047A59	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-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 49 fd 02 fd 5a 53 62 4f fd 2a 47 0b 18 38 80 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 87 70 fd fd 46 47 fd fd fd 2b 40 fd 48 fd 0b 00 00 00 00 00 00 00 64 13 fd fd fd 24 2f 48 fd 1d fd 10 4e 0f fd 2d 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	MeFyzIZSbO*G8S,XFFaqpFG+@Hd$/HN-P>PBxxxx+	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	fd 87 70 fd fd 46 47 fd fd fd 2b 40 fd 48 fd 0b 00 00 00 00 00 00 00 64 13 fd fd fd 24 2f 48 fd 1d fd 10 4e 0f fd 2d	pFG+@Hd$/HN-	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.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 23 36 12 29 fd fd 42 fd 53 65 21 0b 37 fd 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 1a 15 2d 54 fd 7e fd 4c fd 42 77 fd 4a 09 0c 1a 01 00 00 00 0e 00 00 00 00 00 00 00 77 2f 18 3c 68 fd 64 4c fd fd 58 fd 35 60 47 fd 01 00 00 00 06 20 fd fd fd fd 43 19 7d 09 6f 49 fd 6a fd fd 46 05 fd 4f 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 71 30 20 58 6a fd 45 fd fd 5a fd 03 fd 79 17 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	zV#6)BSe!70MMCOYpe-T~LBwJw/<hdLX5`GC}oIjFOJRwpsq0 XjEZy	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	14904	122	ea 69 49 01 0c 56 0c 23 36 12 29 fd fd 42 fd 53 65 21 0b 37 fd fd fd 57 77 3d fd 69 38 fd 4f fd 54 fd 56 40 fd 49 37 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 71 30 20 58 6a fd 45 fd fd 5a fd 03 fd 79 17 05	iIV#6)BSe!7Ww=i8OTV@I7` 8fJRwpsJRwpsq0 XjEZy	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	10824	56	03 10 fd fd 06 00 fd 23 36 12 29 fd fd 42 fd 53 65 21 0b 37 fd 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	#6)BSe!70MMCOYpe	success or wait	4	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 49 fd 02 fd 5a 53 62 4f fd 2a 47 0b 18 38 80 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 87 70 fd fd 46 47 fd fd fd 2b 40 fd 48 fd 0b 00 00 00 00 00 00 00 64 13 fd fd fd 24 2f 48 fd 1d fd 10 4e 0f fd 2d 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	MeFyzIZSbO*G8S,XFFaqpFG+@Hd$/HN-P>PBxxxx+	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	fd 87 70 fd fd 46 47 fd fd fd 2b 40 fd 48 fd 0b 00 00 00 00 00 00 00 64 13 fd fd fd 24 2f 48 fd 1d fd 10 4e 0f fd 2d	pFG+@Hd$/HN-	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	15208	134	ea 69 49 01 0c 56 0c fd fd 43 19 7d 09 6f 49 fd 6a fd fd 46 05 fd 4f fd fd 76 fd fd 51 fd 7d 49 fd fd fd 15 01 fd 1b 1d 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd fd fd 2a 6f 6d fd fd 4d fd 64 fd 57 3c 4a fd fd 01 00 00 11 03 39 03 00 75 fd 00 fd 60 03 0c 66 37 fd 67 fd fd 19 41 fd 49 16 fd fd 3e 5c fd 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	iIVC}oIjFOvQ}I2*omMdW<J9u`f7gAI>\9N8I[Eby	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	15344	70	ea 69 49 01 0c 56 1c fd fd 43 19 7d 09 6f 49 fd 6a fd fd 46 05 fd 4f fd fd 76 fd fd 51 fd 7d 49 fd fd fd 15 01 fd 1b 1d 04 00 00 00 00 00 00 00 07 58 22 0c 77 2f 18 3c 68 fd 64 4c fd fd 58 fd 35 60 47 fd 05	iIVC}oIjFOvQ}IX"w/<hdLX5`G	success or wait	4	7FEE9047A59	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-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	2804	298	05 fd 00 fd 6d 07 11 fd fd 43 19 7d 09 6f 49 fd 6a fd fd 46 05 fd 4f 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 fd fd 43 19 7d 09 6f 49 fd 6a fd fd 46 05 fd 4f 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 1a 15 2d 54 fd 7e fd 4c fd 42 77 fd 4a 09 0c 1a 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 51 fd fd 63 fd 07 fd 4f fd 3a fd fd fd fd 54 fd 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 5e 42 5c 58 03 fd fd 48 fd 3b fd 4a fd fd fd fd 01 00 00 00 05 fd 00 fd fd 07 19 50 fd 34 63 fd fd fd 4b fd fd 70 64 08 fd 6f 59 01 00 00 00 01 01 00 10	mC}oIjFO~C}oIjFO-T~LBwJQcO:T`^ B\XH;JP4cKpdoY	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 49 fd 02 fd 5a 53 62 4f fd 2a 47 0b 18 38 80 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 87 70 fd fd 46 47 fd fd fd 2b 40 fd 48 fd 0b 00 00 00 00 00 00 00 64 13 fd fd fd 24 2f 48 fd 1d fd 10 4e 0f fd 2d 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	MeFyzIZSbO*G8S,XFFaqpFG+@Hd$/HN-P>PBxxxx+	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	fd 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12	J@BH)%5VJ	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	19456	130	ea 69 49 01 0c 56 0c 48 50 05 fd 3f fd fd 4b fd fd 3e 21 4d 46 fd 40 1c 6d 2b fd 1e fd 63 45 fd 18 fd 22 20 fd fd fd 03 00 00 00 00 00 00 00 0b fd 00 fd 2a 0c fd fd 5e fd 7e fd 74 4a fd fd fd fd 7e 50 fd 0a 03 39 03 00 75 fd 00 fd 60 03 0c 55 17 fd 06 25 48 fd 42 fd fd fd fd 0b 03 11 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	iIVHP?K>!MFm+cE" *^~tJ~P9u`U%H B95OKOqy	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	19704	70	ea 69 49 01 0c 56 24 48 50 05 fd 3f fd fd 4b fd fd 3e 21 4d 46 fd 40 1c 6d 2b fd 1e fd 63 45 fd 18 fd 22 20 fd fd fd 06 00 00 00 00 00 00 00 07 58 22 0c 6e 48 57 fd fd 43 fd fd 2b 3c fd c4 18 05	iIV$HP?K>!MFm+cE" X"nWC+<	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	19904	690	3e 03 00 00 54 07 00 00 00 fd 54 fd 0c fd fd fd 72 5d fd fd 42 fd 3c 00 fd 63 fd fd 3a fd 09 0c 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 14 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 1c 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 24 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 7a 03 00 00 58 2b 29 0c 18 fd fd 7d fd 36 4a fd 23 fd 0f fd fd 5a fd 01 00 00 00 fd 54 27 0c 5f fd fd fd fd fd 5f 48 fd fd 46 4a 58 fd 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 42 52 fd fd 13 fd 4c 42 fd b1 fd 78 fd fd 79 01 00 00 00 fd 54 27 0c 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 19 00 fd 03 00 00 fd 54 27 14 29 5b fd 14 76 fd fd 40 fd 6f fd 33 7c fd fd 41 39 00 fd 03 00 00 fd 54 27 1c 29 5b fd 14	>TTr]B<c:)[v@o3|A) [v@o3|A)[v@o3|A$) [v@o3|AzX+)}6J#ZT'__H JXyj XSQJRwpsBRLBxyT') [v@o3|AT')[v@o3|A9T')[	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	3674	372	05 fd 00 fd fd 09 11 48 50 05 fd 3f fd fd 4b fd fd 3e 21 4d 46 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 fd 00 00 00 00 05 fd 00 fd fd 09 0e 48 50 05 fd 3f fd fd 4b fd fd 3e 21 4d 46 fd fd 02 00 00 00 01 01 00 21 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 09 48 50 05 fd 3f fd fd 4b fd fd 3e 21 4d 46 fd fd 04 00 00 00 01 02 00 22 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 10 fd fd 6b fd fd fd 42 fd fd ac 40 79 fd fd 01 00 00 00 01 03 00 23 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 57 44 29 46 fd fd 32 43 45 fd 79 1d 34 07 fd 71 3d 01 00 00 00 01 06 00 24 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd 00 00 00 00 07 60 fd fd fd	HP?K>!MF HP? K>!MF!HP?K>!MF"kB@ y#WD)F2CEy4q=$`	success or wait	3	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.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	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 4d fd 09 37 fd fd 2b 4d fd fd 11 fd 4c fd fd 4e 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 13 4a fd fd fd fd 40 fd 42 fd 48 fd fd fd 0f 00 00 00 00 00 00 00 fd fd 29 fd 25 35 56 4a fd fd 07 20 fd fd fd 12 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	MeFyzM7+MLNS,XFFaq J@BH)%5VJ SWxxxx*	success or wait	1	7FEE9047A59	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{5048B624-CC25-47D4-B88B-9B5A8E4583C5}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	19	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	1	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE9047AFD	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	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	0	512	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{6806B3C0-D11D-4BCE-84B7-B2587F6807DC}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEE9047AFD	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	7FEE9047AFD	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	7FEE9047AFD	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	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	19	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	16	1	success or wait	1	7FEE9047AFD	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	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	19	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	success or wait	1	7FEE9047AFD	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	7FEE9047AFD	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	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	0	512	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	0	512	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\Desktop\C1ZGt61uGv.docx	3015	322	success or wait	1	6E250648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AC592AE0.emf	unknown	8192	success or wait	2	6E250648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AC592AE0.emf	unknown	8192	end of file	1	6E250648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AC592AE0.emf	unknown	8192	success or wait	2	6E250648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AC592AE0.emf	unknown	8192	end of file	1	6E250648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AC592AE0.emf	unknown	22	success or wait	1	6E250648	unknown
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{ECAF6FF3-F9CF-495B-80DB-8035DEA309E7}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{82D6D04A-E2A7-42F1-89A6-CFD57F9EC766}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E22A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E22A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E22A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E250648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E250648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E250648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\7472E	success or wait	1	6E250648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\7472E	7472E	binary	04 00 00 00 90 0B 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	success or wait	1	6E250648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			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 AF 2B 00 E8 F4 B2 D8 01 2E 47 07 00 2E 47 07 00 00 00 00 00 DB 04 00 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	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 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\00004109D30000000010000 0000F01FEC\Usage	ProductFiles	dword	1427243058	1427243059	success or wait	1	6E250648	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000010000 0000F01FEC\Usage	ProductFiles	dword	1427243059	1427243060	success or wait	1	6E250648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\7472E	7472E	binary	04 00 00 00 90 0B 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 AF 2B 00 E8 F4 B2 D8 01 2E 47 07 00 2E 47 07 00 00 00 00 00 DB 04 00 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 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	04 00 00 00 90 0B 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 2E 47 07 00 2E 47 07 00 00 00 00 00 DB 04 00 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 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	success or wait	1	6E250648	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				

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 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 FF FF FF FF				

Disassembly

No disassembly